

The Honorable Richard A. Jones

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT SEATTLE

NATALIE PERKINS and KENNETH
HASSON, individually and on behalf of
themselves and of all others similarly situated,

Plaintiffs,

v.

ZILLOW GROUP, INC. and MICROSOFT
CORPORATION,

Defendants.

NO. 2:22-cv-01282

**ZILLOW GROUP, INC.’S NOTICE
OF FILING OF MOTION TO
TRANSFER ACTIONS –
28 U.S.C. § 1407**

Defendant Zillow Group, Inc. (“Zillow”), by and through its undersigned counsel,
hereby files a copy of Zillow’s Motion to Transfer Actions Pursuant to 28 U.S.C. § 1407 for
Coordinated or Consolidated Pretrial Proceedings pursuant to United States Panel on
Multidistrict Litigation Rule of Procedure 6.2(a). The Motion is filed contemporaneously as
Exhibit A.

1 DATED: October 24, 2022.

2 **SAVITT BRUCE & WILLEY LLP**

3 By s/ James P. Savitt

4 James P. Savitt, WSBA # 16847
5 1425 Fourth Avenue Suite 800
6 Seattle, Washington 98101-2272
7 Telephone: 206.749.0500
8 Facsimile: 206.749.0600
9 Email: jsavitt@sbwllp.com

10 **OF COUNSEL:**

11 **BUCHANAN INGERSOLL & ROONEY PC**

12 Samantha L. Southall (*pro hac vice* forthcoming)
13 50 South 16th Street Suite 3200
14 Philadelphia, PA 19102
15 Telephone: 215-665-8700
16 Facsimile: 215-665-8760
17 Email: samantha.southall@bipc.com

18 *Attorneys for Defendant Zillow Group, Inc.*

CERTIFICATE OF SERVICE

The undersigned hereby certifies that, on October 24, 2022, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system which will send notification of such filing to all counsel of record.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

EXECUTED this 24th day of October, 2022 at Seattle, Washington.



Meghan Parker

Exhibit A

Time-stamped copy of Zillow
Group, Inc.'s Motion to
Transfer Actions Pursuant to 28
U.S.C. § 1407 for Coordinated
or Consolidated Pretrial
Proceedings

**BEFORE THE
UNITED STATES JUDICIAL PANEL
ON MULTIDISTRICT LITIGATION**

**In re: ZILLOW GROUP, INC. SESSION
REPLAY SOFTWARE LITIGATION**

MDL-__

**MOTION TO TRANSFER ACTIONS PURSUANT TO 28 U.S.C. § 1407 FOR
COORDINATED OR CONSOLIDATED PRETRIAL PROCEEDINGS**

Defendant Zillow Group, Inc. (“Zillow”) respectfully requests, pursuant to 28 U.S.C. § 1407(a) and the United States Judicial Panel on Multidistrict Litigation Rule of Procedure 6.2, that this Panel issue an order for transfer and consolidation for the eight civil actions listed in the Schedule of Actions (“the Actions”) filed concurrently herewith.

For the reasons set forth in the accompanying Brief in Support of its Motion, it is appropriate and necessary pursuant to 28 U.S.C. § 1407 for the Panel to issue an order transferring and consolidating the Actions listed in the accompanying Schedule of Actions, as well as all subsequently filed related actions, to the United States District Court Western District of Washington for coordinated or consolidated pretrial proceedings.

Dated: October 19, 2022

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

By: /s/ Samantha L. Southall

Samantha L. Southall

Two Liberty Place

50 S. 16th Street, Suite 3200

Philadelphia, Pennsylvania 19102

(215) 665-8700

samantha.southall@bipc.com

Christopher J. Dalton
550 Broad Street, Suite 810
Newark, New Jersey 07102-4582
(973) 273-9800
christopher.dalton@bipc.com

Jennifer Olmedo-Rodriguez
One Biscayne Tower
2 S. Biscayne Blvd., Suite 1500
Miami, Florida 33131
(305) 347-5900
jennifer.olmedo-rodriguez@bipc.com

Counsel for Zillow Group, Inc.

**BEFORE THE
UNITED STATES JUDICIAL PANEL
ON MULTIDISTRICT LITIGATION**

**In re: ZILLOW GROUP, INC. SESSION
REPLAY SOFTWARE LITIGATION**

MDL-__

**ZILLOW GROUP, INC.'S BRIEF IN SUPPORT OF MOTION TO TRANSFER
ACTIONS PURSUANT TO 28 U.S.C. § 1407 FOR
COORDINATED OR CONSOLIDATED PRETRIAL PROCEEDINGS**

BUCHANAN INGERSOLL & ROONEY PC

By: Samantha L. Southall
Two Liberty Place
50 S. 16th Street, Suite 3200
Philadelphia, Pennsylvania 19102
(215) 665-8700
samantha.southall@bipc.com

By: Christopher J. Dalton
550 Broad Street, Suite 810
Newark, New Jersey 07102-4582
(973) 273-9800
christopher.dalton@bipc.com

By: Jennifer Olmedo-Rodriguez
One Biscayne Tower
2 S. Biscayne Blvd., Suite 1500
Miami, Florida 33131
(305) 347-5900
jennifer.olmedo-rodriguez@bipc.com

Counsel for Zillow Group, Inc.

TABLE OF CONTENTS

	Page
INTRODUCTION	1
BACKGROUND	2
ARGUMENT	6
I. Transfer is Appropriate Under 28 U.S.C § 1407.	6
A. The Actions Involve Identical Factual Issues.	8
B. Transfer Will Serve The Convenience Of The Parties, Witnesses, And Counsel.	9
C. Transfer Will Promote The Just And Efficient Conduct Of The Actions.....	11
D. The Actions Are Sufficiently Numerous And Complex To Warrant Consolidation.	12
II. The Western District of Washington Is The Most Appropriate Transferee Forum.	13
CONCLUSION.....	15

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>In re Aetna, Inc.</i> , 609 F. Supp. 2d 1370 (J.P.M.L. 2009).....	13
<i>In re Air Crash Disaster at Huntington, W. Va. on Nov. 14, 1970</i> , 342 F. Supp. 1400 (J.P.M.L. 1972).....	9
<i>In re Air West, Inc. Sec. Litig.</i> , 384 F. Supp. 609 (J.P.M.L. 1974).....	8
<i>In re Allura Fiber Cement Siding Prods. Liab. Litig.</i> , 366 F. Supp. 3d 1365 (J.P.M.L. 2019).....	12
<i>In re Azek Bldg. Prods.</i> , 999 F. Supp. 2d 1366 (J.P.M.L. 2014).....	12
<i>In re Bair Hugger Forced Air Warming Devices Prods. Liab. Litig.</i> , 148 F. Supp. 3d 1383 (J.P.M.L. 2015).....	14
<i>In re Bard IVC Filters Prods. Liab. Litig.</i> , 122 F. Supp. 3d 1375 (J.P.M.L. 2015).....	14
<i>In re Chrysler Pacifica Fire Recall Prods. Liab. Litig.</i> , MDL No. 3040, 2022 WL 3134131 (J.P.M.L. Aug. 3, 2022)	12
<i>In re Clearview AI, Inc. Consumer Privacy Litig.</i> , 509 F. Supp. 3d 1368 (J.P.M.L. 2020).....	7, 13
<i>In re Equifax, Inc., Customer Data Sec. Breach Litig.</i> , 289 F. Supp. 3d 1322 (J.P.M.L. 2017).....	14
<i>In re Facebook Internet Tracking Litig.</i> , 844 F. Supp. 2d 1374 (J.P.M.L. 2012).....	7
<i>In re Facebook, Inc., Consumer Privacy User Profile Litig.</i> , 325 F. Supp. 3d 1362 (J.P.M.L. 2018).....	13, 14
<i>In re Fed. Election Campaign Act Litig.</i> , 511 F. Supp. 821 (J.P.M.L. 1979).....	8
<i>In re FedLoan Student Loan Servicing Litig.</i> , 340 F. Supp. 3d 1377 (J.P.M.L. 2018).....	14

<i>In re First Nat'l Bank, Heavener, Okla. (First Mortgage Revenue Bonds) Sec. Litig.,</i> 451 F. Supp. 995 (J.P.M.L. 1978).....	13
<i>In re Google Inc. Cookie Placement Consumer Privacy Litig.,</i> 867 F. Supp. 2d 1356 (J.P.M.L. 2012).....	7
<i>In re Google Inc. Gmail Litig.,</i> 936 F. Supp. 2d 1381 (J.P.M.L. 2013).....	9, 13
<i>In re Johnson & Johnson Talcum Powder Prod. Mktg., Sales Practices & Prod. Liab. Litig.,</i> 220 F. Supp. 3d 1356 (J.P.M.L. 2016).....	11
<i>In re Lehman Bros. Hldg., Inc.,</i> 598 F. Supp. 2d 1362 (J.P.M.L. 2009).....	10
<i>In re Lenovo Adware Litig.,</i> 109 F. Supp. 3d 1366 (J.P.M.L. 2015).....	14
<i>In re Neo Wireless, LLC, Pat. Litig.,</i> MDL No. 3034, 2129058 (J.P.M.L. June 14, 2022)	12
<i>In re Nickelodeon Consumer Privacy Litig.,</i> 949 F. Supp. 2d 1377 (J.P.M.L. 2013).....	7, 12
<i>In Re Nifedipine,</i> 266 F. Supp. 2d 1382 (J.P.M.L. 2003).....	6
<i>In re Okun,</i> 609 F. Supp. 2d 1380 (J.P.M.L. 2009).....	13
<i>In re Packaged Seafood Prods. Antitrust Litig.,</i> 148 F. Supp. 3d 1375 (J.P.M.L. 2015).....	14
<i>In re Payless ShoeSource, Inc.,</i> 609 F. Supp. 2d 1372 (J.P.M.L. 2009).....	13
<i>In re Phenylpropanolamine Prod. Liab. Litig.,</i> 460 F.3d 1217 (9th Cir. 2006)	7
<i>In re Samsung Top-Load Washing Machine Mktg., Sales Practices and Prods. Liab. Litig.,</i> 278 F. Supp. 3d 1376 (J.P.M.L. 2017).....	9
<i>In re Smitty's/Cam2 303 Tractor Hydraulic Fluid Mktg., Sales Practices & Prods. Liab. Litig.,</i> 466 F. Supp. 3d 1380 (J.P.M.L. 2020).....	12

<i>In re Sony Corp. SXRD Rear Projection TV Mktg. Sales Practices & Prods. Liab. Litig.</i> , 655 F. Supp. 2d 1367 (J.P.M.L. 2009).....	10
<i>In re TikTok, Inc., Consumer Privacy Litig.</i> , 481 F. Supp. 3d 1331 (J.P.M.L. 2020).....	7
<i>In re Toyota Motor Corp. Hybrid Brake Mktg., Sales Practices, & Prod. Liab. Litig.</i> , 732 F. Supp. 2d 1375 (J.P.M.L. 2010).....	14
<i>In re Transocean Ltd. Sec. Litig. (No. II)</i> , 753 F. Supp. 2d 1373 (J.P.M.L. 2010).....	12
<i>In re Travel Agent Comm’n Antitrust Litig.</i> , 290 F. Supp. 2d 1381 (J.P.M.L. 2003).....	8
<i>In re Vizio, Inc., Consumer Privacy Litig.</i> , 176 F. Supp. 3d 1374 (J.P.M.L. 2016).....	7, 10
Statutes	
28 U.S.C. § 1407.....	<i>passim</i>
Rules	
Multidistrict Litigation Rule of Procedure 6.2.....	1

Defendant Zillow Group, Inc. (“Zillow”), by and through undersigned counsel, respectfully submits this brief in support of its motion pursuant to 28 U.S.C. § 1407 and the United States Judicial Panel on Multidistrict Litigation Rule of Procedure 6.2 for the transfer of certain actions to the United States District Court for the Western District of Washington for coordinated or consolidated pretrial proceedings.

INTRODUCTION

Plaintiffs in five different states have filed eight putative class actions in six separate federal district courts across the country, each alleging that Zillow violated various states’ wiretapping statutes and committed common law privacy torts through the alleged use of technology purportedly embedded on its desktop and mobile websites (collectively, the “Actions”). This panel should transfer and assign the pending Actions listed in the Schedule of Actions to the United States District Court for the Western District of Washington – as well as any subsequently filed similar actions – because each action arises from the same substantive factual allegations and asserts nearly identical legal theories of recovery. In addition, each action is in a nascent stage: Zillow has not yet responded to any of the eight complaints, nor has discovery commenced.

More specifically, each Action arises from Plaintiffs’ alleged interaction with snippets of JavaScript computer code (“Session Replay Code”) purportedly embedded on Zillow’s desktop and mobile websites which, Plaintiffs contend, “deploys on each website visitor’s internet browser for the purpose of intercepting and recording the website visitor’s electronic communications with the Zillow website, including their [sic] mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic

communications in real-time (“Website Communications”).”¹ The Actions all seek similar relief on behalf of Zillow desktop and mobile website visitors whose website communications were allegedly “captured” or “intercepted” through the use of Session Replay Code.

The Western District of Washington is the most appropriate district within which to consolidate these substantively identical Actions because it is where Zillow is headquartered, where many witnesses are likely to be located, and where, as one complaint alleges, “a substantial part of the events and conduct giving rise to Plaintiffs’ claims occurred.” *See Perkins* Compl. at ¶ 10. Moreover, Zillow’s Terms of Use, which are disclosed to the public, identify the state and federal courts in King County, Washington as the exclusive venue for all disputes arising from Plaintiffs’ use of the websites. *Id.* at ¶ 80. Because of the nature of Zillow’s business, including its nationwide virtual footprint and its usage by individuals in multiple (and, perhaps, all) states, additional cases filed in the future should also be consolidated in the Western District of Washington.

BACKGROUND

Zillow was founded and is headquartered in Seattle, Washington, first launching its website in 2006. As the most-visited real estate website in the United States, Zillow’s companies offer users an on-demand experience for selling, buying, renting, and financing properties with

¹ This exact language appears in six of the eight complaints. *See Margulis v. Zillow Group, Inc.*, No. 1:22-cv-04847 (Sep. 8, 2022) (N.D. Ill.); *Popa v. Zillow Group, Inc.*, No. 2:22-cv-01287 (Sep. 8, 2022) (W.D. Pa.); *Perkins v. Zillow Group, Inc.*, No. 2:22-cv-01282 (Sep. 12, 2022) (W.D. Wash.); *Strelzin v. Zillow Group, Inc.*, No. 1:22-cv-05644 (Sep. 15, 2022) (N.D. Ill.); *Conlisk v. Zillow Group, Inc.*, No. 1:22-cv-05082 (Sep. 19, 2022) (N.D. Ill.); *Adams v. Zillow Group, Inc.*, No. 4:22-cv-01023 (Sep. 27, 2022) (E.D. Mo.). The other two complaints contain identical contentions that Zillow uses “‘session replay’ spyware to intercept Plaintiff’s and the Class members’ electronic computer-to-computer data communications with Defendant’s website, including how they interacted with the website, their mouse movements and clicks, keystrokes, search terms, information inputted into the website, and pages and content viewed while visiting the website.” *See Huber v. Zillow Group, Inc.*, No. 2:22-cv-03572 (Sep. 7, 2022) (E.D. Pa.); *Kauffman v. Zillow Group, Inc.*, No. 3:22-cv-01398 (Sep. 15, 2022) (S.D. Cal.).

transparency and nearly seamless end-to-end service.

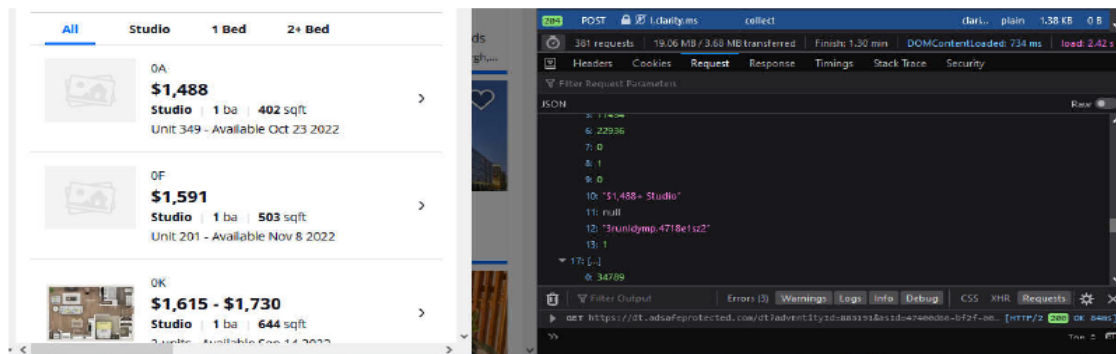
On September 7, 2022, Plaintiff Jamie Huber filed a putative class action in the United States District Court for the Eastern District of Pennsylvania alleging that Zillow improperly utilized Session Replay Code to “intercept . . . electronic computer-to-computer data communications,” and in doing so, purportedly storing and recording website visitors’ information without the visitors’ knowledge or prior consent. *Huber* Compl. at ¶ 3. Huber claims that Zillow’s alleged interception and capture of her interactions with the Zillow website “through her computer and/or mobile device” by the Session Replay Code violate the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Cons. Stat. § 5701 *et seq.* (“WESCA”). *Id.* at ¶¶ 26, 37, 75-87.

Between September 7 and September 27, 2022 – a mere twenty days –seven more nearly identical putative class action complaints were filed in six additional courts, sometimes by some of the same lawyers. Those actions are:

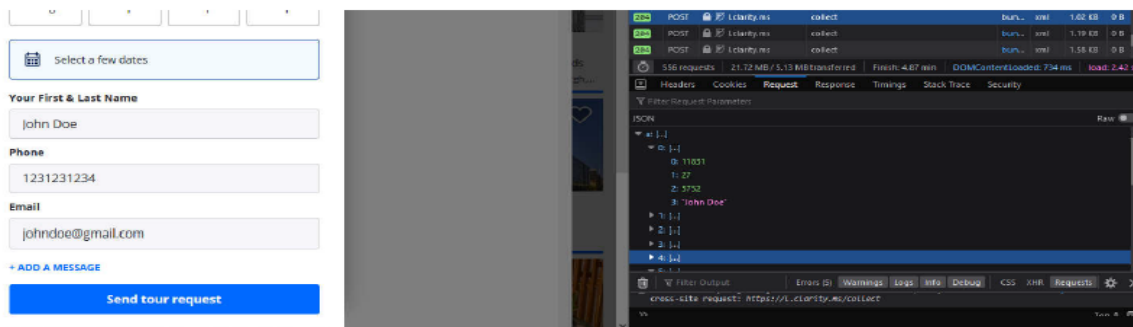
CASE NAME	JURISDICTION	DATE FILED
<i>Popa v. Zillow Group, Inc.</i> Case No. 2:22-cv-01287	W.D. Pennsylvania	9/8/2022
<i>Margulis v. Zillow Group, Inc.</i> Case No. 1:22-cv-04847	N.D. Illinois	9/8/2022
<i>Perkins v. Zillow Group, Inc. and Microsoft Corp.</i> Case No. 2:22-cv-01282	W.D. Washington	9/12/2022
<i>Kauffman v. Zillow Group, Inc.</i> Case No. 3:22-cv-01398	S.D. California	9/15/2022
<i>Strelzin v. Zillow Group, Inc.</i> Case No. 1:22-cv-05644	Cook County Circuit Court (filed) N.D. Illinois (removed)	9/15/2022 (filed) 10/14/2022 (removed)
<i>Conlisk v. Zillow Group, Inc.</i> Case No. 1:22-cv-05082	N.D. Illinois	9/19/2022
<i>Adams v. Zillow Group, Inc.</i> Case No. 4:22-cv-1023	E.D. Missouri	9/27/2022

In each of the complaints, the common factual allegations regarding Zillow’s use of Session Replay Code are largely indistinguishable and, in some instances, identical. The sameness

of these Actions is perhaps best demonstrated by the fact that six of the eight Actions use *identical* screenshots and descriptions that depict “information sent to one of the Service Replay Providers—Microsoft – through a Session Replay Code – Clarity – after viewing a Studio apartment priced at \$1,488 while visiting www.zillow.com” and “after entering a name (purple text) to a text box to schedule a tour of a property”:



Depicting information sent to one of the Service Replay Providers—Microsoft—through a Service Replay Code—Clarity—after viewing a Studio apartment priced at \$1,488 while visiting www.zillow.com.



Depicting information sent to one of the Service Replay Providers—Microsoft—through a Service Replay Code—Clarity—after entering a name (purple text) to a text box to schedule a tour of a property.

Not only are these screenshots and descriptions identical – they are found at the exact same location within the six complaints that utilize them. *See Margulis* Compl. at ¶¶ 49-50; *Conlisk* Compl. at ¶¶ 51-52; *Perkins* Compl. at ¶¶ 61-62; *Popa* Compl. at ¶¶ 48-49; *Strelzin* Compl. at ¶¶ 49-50; and

Adams Compl. at ¶¶ 51-52.²

Plaintiffs’ theories of recovery are also nearly identical. Each action asserts a civil claim for violation of a state wiretapping law. *See Huber* Compl. at ¶ 2 and *Popa* Compl. at ¶ 3 (WESCA); *Margulis* Compl. at ¶ 3, *Conlisk* Compl. at ¶ 4, and *Strelzin* Compl. at ¶ 3 (Illinois Eavesdropping Act, 720 ILCS 5/14-1, *et seq.*); *Kauffman* Compl. at ¶ 1 (California Penal Code § 631, (“CIPA”)); *Adams* Compl. at ¶ 3 (Missouri Wiretap Act, Mo. Ann. Stat. §§ 542.400 *et seq.*); *Perkins* Compl. at ¶ 3 (Washington Wiretapping Statute, Wash. Rev. Code § 9.73.030 *et seq.*). Seven of the Actions also assert a tort claim for invasion of privacy, and four Actions assert claims for violation of consumer protection laws. *Margulis* Compl. at ¶ 3, *Conlisk* Compl. at ¶4, and *Strelzin* Compl. at ¶ 3 (Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.*); *Adams* Compl. at ¶ 3 (Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.010 *et seq.*).

Moreover, each Plaintiff seeks to represent a putative class of persons whose communications were “intercepted” or “captured through the use of Session Replay Code embedded in www.zillow.com.” *See Huber* Compl. at ¶ 64; *Popa* Compl. at ¶ 56; *Margulis* Compl. at ¶ 57; *Conlisk* Compl. at ¶ 59; *Strelzin* Compl. at ¶ 57; *Kauffman* Compl. at ¶ 57; *Adams* Compl. at ¶¶ 59-60; *Perkins* Compl. at ¶ 69.

While seven of the eight complaints seek to certify classes of state residents, the *Perkins* action pending in the Western District of Washington asserts claims on behalf of a putative nationwide class.³ In seven of the eight Actions, Zillow is the sole defendant, and Microsoft, Inc.

² Interestingly, these identical screenshots are used despite the fact that four different sets of lawyers represent these Plaintiffs.

³ The Missouri Action also alleges a putative subclass of “minors” who allegedly visited Zillow’s website. *Adams* Compl. at ¶ 60.

(also located in Washington) is a co-defendant with Zillow in the *Perkins* Action. In the eighth Action (*Perkins*), the only other defendant is Microsoft, Inc., which is also located in Washington. Thus, while the residency of the Plaintiffs vary, the Action with the largest putative class is pending in Washington, and all of the Defendants in all eight Actions are located in Washington.

Critically, all eight Actions are in their infancy. Zillow has not yet responded to any of the complaints; no court has scheduled or conducted an initial pretrial conference pursuant to Fed. R. Civ. P. 16(b); and no discovery has yet commenced.

ARGUMENT

Pursuant to 28 U.S.C. §1407(a), transfer is appropriate where, as here: (1) the cases “involv[e] one or more common questions of fact;” (2) transfer and consolidated or coordinated proceedings will further “the convenience of parties and witnesses;” and (3) transfer and consolidated or coordinated proceedings “will promote the just and efficient conduct of [the] actions.” *See In Re Nifedipine*, 266 F. Supp. 2d 1382, 1382 (J.P.M.L. 2003).

The Actions involve effectively identical factual allegations and legal issues. Transfer will benefit the parties, the witnesses, and the courts. The Actions involve the same desktop and mobile websites, the same allegations about Zillow’s use of Session Replay Code, and virtually identical proposed classes. Further, because Zillow is located in the Western District of Washington and many witnesses are likely to be located in that jurisdiction, transfer to that District is most appropriate. Absent transfer for pretrial proceedings, the parties will incur excessive costs due to duplicative discovery in California, Illinois, Missouri, Pennsylvania, and Washington (at a minimum). They also will face the substantial risk of inconsistent rulings.

I. Transfer is Appropriate Under 28 U.S.C § 1407.

Transfer of the Actions is appropriate and will further the goals of the statute to promote efficiency and consistency. The statute “was meant to assure uniform and expeditious treatment

in the pretrial procedures in multidistrict litigation” and to avoid inconsistent pretrial demands that might “disrupt the functions of the Federal courts.” *In re Phenylpropanolamine Prod. Liab. Litig.*, 460 F.3d 1217, 1230 (9th Cir. 2006) (quotation omitted). Because centralization of the Actions will “eliminate duplicative discovery and the possibility of inconsistent rulings on class certification and other pretrial matters, as well as conserve judicial and party resources,” this Panel should transfer the Actions to the Western District of Washington. *In re TikTok, Inc., Consumer Privacy Litig.*, 481 F. Supp. 3d 1331 (J.P.M.L. 2020).

Centralization of these Actions accords with the Panel’s previous decisions “involving the allegedly unlawful tracking of individuals’ internet activity.” *In re Nickelodeon Consumer Privacy Litig.*, 949 F. Supp. 2d 1377 (J.P.M.L. 2013). Indeed, the Panel has consistently transferred consumer privacy actions similar to this one for coordination. *See, e.g., In re Clearview AI, Inc. Consumer Privacy Litig.*, 509 F. Supp. 3d 1368, 1369 (J.P.M.L. 2020) (claims based on alleged improper collection and distribution or sale of citizens’ biometric data); *In re TikTok, Inc., Consumer Privacy Litig.*, 481 F. Supp. 3d 1331 (J.P.M.L. 2020) (claims based on allegedly improper scanning, capture, retention, and dissemination of facial geometry and other biometric information of app’s users); *In re Vizio, Inc., Consumer Privacy Litig.*, 176 F. Supp. 3d 1374, 1375–76 (J.P.M.L. 2016) (claims based alleged violations of customers’ privacy rights through collection and sharing of Smart TV viewing data); *In re Nickelodeon Consumer Privacy Litig.*, 949 F. Supp. 2d 1377, 1378 (J.P.M.L. 2013) (claims based alleged violations of privacy rights of minor children); *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 867 F. Supp. 2d 1356, 1357 (J.P.M.L. 2012); *In re Facebook Internet Tracking Litig.*, 844 F. Supp. 2d 1374, 1375 (J.P.M.L. 2012) (claims based alleged violations of wiretap laws, Stored Electronic Communications Act, 18 U.S.C. § 2701, CAFA, and common law claims for invasion of privacy,

unjust enrichment, and trespass to chattels).

A. The Actions Involve Identical Factual Issues.

The initial test for transfer and coordination under Section 1407 is the presence of similar questions of fact. *In re Fed. Election Campaign Act Litig.*, 511 F. Supp. 821, 823 (J.P.M.L. 1979). This threshold requirement is satisfied where, as here, “two or more complaints assert comparable allegations against identical defendants based upon similar transactions and events....” *In re Air West, Inc. Sec. Litig.*, 384 F. Supp. 609, 611 (J.P.M.L. 1974).

The alleged conduct underlying the Actions consists of nearly identical factual assertions arising from nearly identical events: that Zillow allegedly deploys snippets of JavaScript computer code referred to as “Session Replay Code” from its desktop and mobile websites onto each website visitor’s internet browser; that it purportedly does so for the purpose of intercepting and recording each website visitor’s private electronic communications without their consent; and that each Plaintiff was allegedly harmed by visiting Zillow’s website. The factual questions to be adjudicated will include, but are not limited to, whether: (1) Zillow’s Session Replay Code “intercepts” website interactions; (2) Zillow used “Session Replay Providers” (such as Microsoft) to intercept and record website interactions; (3) Zillow intentionally disclosed website interactions of its website users to third parties; (4) Zillow disclosed to its users that it was purportedly capturing their website interactions; (5) Plaintiffs consented to the use of Session Replay Code; (6) Plaintiffs had a reasonable expectation of privacy in their activities on the Zillow.com website; (7) users’ website interactions constitute “communications”; and (8) Session Replay Code is an “eavesdropping device”.

Any differences in the factual allegations of each case are minimal at best and do not negate that transfer is proper pursuant to Section 1407. *See In re Travel Agent Comm’n Antitrust Litig.*, 290 F. Supp. 2d 1381, 1382 (J.P.M.L. 2003) (“Section 1407 does not require a complete identity

or even [a] majority of common factual and legal issues as a prerequisite to centralization.”); *cf. In re Samsung Top-Load Washing Machine Mktg., Sales Practices and Prods. Liab. Litig.*, 278 F. Supp. 3d 1376, 1378 (J.P.M.L. 2017) (granting motion as to an action that focused on one component of the product in question where the other MDL actions focused on various components of the product). As discussed above, but for minor variations specific to the individual Plaintiffs, the complaints in the Actions are all but identical.

The Actions likewise involve similar legal theories. These will require adjudication of whether Zillow engaged in, among other things, invasion of consumers’ common law privacy rights, violations of various states wiretapping laws, and violations of state consumer-protection laws in its alleged use of Session Replay Code on its desktop and mobile websites. Although the legal claims differ slightly in each case due to the differing state wiretapping and consumer protection laws invoked, *all* Plaintiffs seek damages and injunctive relief from Zillow for the *same* alleged conduct and the *same* alleged injury. While the Panel has held that “Section 1407 requires the existence of common questions of fact, not common questions of law,” *In re Air Crash Disaster at Huntington, W. Va. on Nov. 14, 1970*, 342 F. Supp. 1400, 1402 (J.P.M.L. 1972), here, the questions of law are quite common as well. Moreover, this Panel has previously held that potential differences between state wiretapping and eavesdropping laws do not preclude consolidation. *See In re Google Inc. Gmail Litig.*, 936 F. Supp. 2d 1381, 1382 (J.P.M.L. 2013) (consolidating class actions against Google where, as here, plaintiffs from various states alleged that defendant’s conduct “amount[ed] to an illegal ‘interception’ or ‘eavesdropping’ under various federal and/or state wiretapping statutes.”)

B. Transfer Will Serve The Convenience Of The Parties, Witnesses, And Counsel.

Centralization under Section 1407 also will “ensure[] that pretrial proceedings will be

conducted in a streamlined manner leading to the just and expeditious resolution of all actions to the overall benefit of the parties.” *In re Lehman Bros. Hldg., Inc.*, 598 F. Supp. 2d 1362, 1364 (J.P.M.L. 2009). Transfer of multiple actions to a single forum prevents duplication of efforts and eliminates the possibility of overlapping or inconsistent determinations by courts of coordinate jurisdiction. *See In re Vizio, Inc., Consumer Privacy Litig.*, 176 F. Supp. 3d 1374, 1375–76 (J.P.M.L. 2016); *In re Sony Corp. SXRDRear Projection TV Mktg. Sales Practices & Prods. Liab. Litig.*, 655 F. Supp. 2d 1367 (J.P.M.L. 2009). Consolidating the Actions into a single centralized and coordinated pretrial program will further the statute’s goals of fairness and efficiency.

Consolidation will also serve to minimize the inconvenience, inefficiencies, and expense of redundant and duplicative discovery – precisely the purpose of transfer and coordination under Section 1407. Written discovery and witnesses to be deposed will undoubtedly be largely identical in each of the eight Actions. Transfer to Western District of Washington – where the *Perkins* matter is already pending and where Zillow (and Microsoft) are headquartered – will be more convenient for the parties, witnesses, and counsel. To the extent that non-parties are also witnesses or possess potentially responsive evidence, coordination and consolidation benefits them, too. Indeed, without transfer, Zillow will be forced to defend itself in at least six different federal courts for the same legal claims arising from the same factual allegations.

Moreover, each of the Actions – filed in California, Illinois, Missouri, Pennsylvania, and Washington – should have been filed in the United States District Court for the Western District of Washington in the first place, as the Zillow website Terms of Use – which are disclosed to the public, and to which the website’s users are subject – are governed by the laws of the State of Washington:

Choice of Law; Disputes. These Terms of Use are governed by the laws of the State of Washington, without giving effect to its conflict

of laws provisions. You agree to submit to the personal and exclusive jurisdiction and venue in the state and federal courts sitting in King County, Washington for all disputes, claims, and actions arising from or in connection with the Services or otherwise under these Terms of Use. The Zillow Companies operate the Services from our offices in Washington, and we make no representation that the Services are appropriate or available for use in other locations.⁴

Thus, the Western District of Washington is not only the most convenient forum, it is the only appropriate one.⁵

C. Transfer Will Promote The Just And Efficient Conduct Of The Actions.

In addition, transfer of the Actions for coordinated pretrial proceedings will “promote the just and efficient conduct of [the] actions” in accordance with the third requirement of Section 1407(a). Because the Actions were only commenced last month, consolidation will maximize efficiencies and expedite the resolution of the issues in each case. *See In re Johnson & Johnson Talcum Powder Prod. Mktg., Sales Practices & Prod. Liab. Litig.*, 220 F. Supp. 3d 1356, 1358 (J.P.M.L. 2016) (granting consolidation where nearly all the actions were filed within a six-month period). Indeed, the Actions will involve many of the same pretrial issues, such as those concerning the nature and scope of fact discovery, resolution of expert discovery issues and *Daubert* motions, and resolution of legal issues and affirmative defenses at summary judgment. For example, if the Southern District of California, the Northern District of Illinois, the Eastern District of Missouri, the Eastern and Western Districts of Pennsylvania, and the Western District

⁴ <https://www.zillowgroup.com/terms-of-use/> (last visited 10/19/2022).

⁵ The *Perkins* action plaintiffs further allege that “Washington, which seeks to protect the rights and interests of Washington and other U.S. consumers against a company doing business in Washington, has a greater interest in the claims of Plaintiffs and the Class than any other state and is most intimately concerned with the outcome of this litigation.” *Perkins* Compl. at ¶ 81. Given that the *Perkins* plaintiffs seek a nationwide class, this statement is clearly intended to influence a choice-of-law analysis applying Washington law nationwide – with which Zillow disagrees – but nevertheless shows that Washington is the center of gravity here.

of Washington were independently required to each resolve pre-trial issues relating to the overlapping factual record, valuable judicial resources would be wasted and there would be an exceptionally high risk of inconsistent discovery, summary judgment, class allegation, and certification rulings. *See In re Clearview AI, Inc., Consumer Privacy Litig.*, 509 F. Supp. 3d 1368, 1369 (J.P.M.L. 2020); *In re Allura Fiber Cement Siding Prods. Liab. Litig.*, 366 F. Supp. 3d 1365 (J.P.M.L. 2019); *In re Nickelodeon Consumer Privacy Litig.*, 949 F. Supp. 2d 1377, 1378 (J.P.M.L. 2013). This outcome would be unfair to both Plaintiffs and Zillow alike and would burden the court system by creating inefficient procedure and potentially conflicting precedent.

D. The Actions Are Sufficiently Numerous And Complex To Warrant Consolidation.

There are currently eight cases pending in six separate courts in five different states filed within twenty days of each other. There remains the distinct possibility that others will be filed. While there is no “magic number” of pending cases required to grant consolidation under Section 1407, the eight Actions here involve sufficient number of mutual issues and complexities to warrant consolidation.

As a starting point, the Panel regularly centralizes actions where six or more early-stage actions are pending across multiple jurisdictions.⁶ *See, e.g., In re Chrysler Pacifica Fire Recall Prods. Liab. Litig.*, MDL No. 3040, 2022 WL 3134131 (J.P.M.L. Aug. 3, 2022) (seven actions in four districts); *In re Neo Wireless, LLC, Pat. Litig.*, MDL No. 3034, 2129058 (J.P.M.L. June 14, 2022) (seven actions in five districts); *In re Smitty’s/Cam2 303 Tractor Hydraulic Fluid Mktg.*,

⁶ “[W]here only a minimal number of actions are involved,” a party requesting centralization may bear a heavier burden to demonstrate that it is appropriate. However, that heavier burden – utilized in limited circumstances with far fewer actions at issue – does not apply here. *See In re Transocean Ltd. Sec. Litig. (No. II)*, 753 F.Supp.2d 1373, 1374 (J.P.M.L. 2010) (applying heavier burden where there were only two actions); *cf. In re Azek Bldg. Prods.*, 999 F.Supp.2d 1366 (J.P.M.L. 2014) (transferring one case into the District of New Jersey for consolidation).

Sales Practices & Prods. Liab. Litig., 466 F. Supp. 3d 1380 (J.P.M.L. 2020) (eight actions in eight districts); *In re Clearview AI, Inc. Consumer Privacy Litig.*, 509 F. Supp. 3d 1368, 1369 (J.P.M.L. 2020) (nine actions in two districts); *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 325 F. Supp. 3d 1362, 1363 (J.P.M.L. 2018) (eight actions in four districts); *In re Google Inc. Gmail Litig.*, 936 F. Supp. 2d 1381, 1382 (J.P.M.L. 2013) (six actions in five districts).

Additionally, where, as here, the issues involved are sufficiently complex and centralization would prevent duplicative pretrial proceedings and rulings, the Panel has ordered transfer even when as few as two cases were pending. *See, e.g., In re First Nat'l Bank, Heavener, Okla. (First Mortgage Revenue Bonds) Sec. Litig.*, 451 F. Supp. 995, 997 (J.P.M.L. 1978) (centralization was “necessary, even though only two actions are involved, in order to prevent duplicative pretrial proceedings and eliminate the possibility of inconsistent pretrial rulings”); *see also In re Okun*, 609 F. Supp. 2d 1380, 1382 (J.P.M.L. 2009) (centralizing two actions); *In re Payless ShoeSource, Inc.*, 609 F. Supp. 2d 1372 (J.P.M.L. 2009) (same); *In re Aetna, Inc.*, 609 F. Supp. 2d 1370 (J.P.M.L. 2009) (same).

The eight Actions involve related factual issues regarding the same complex technology; each action involves a different set of Plaintiffs asserting effectively identical theories against the same defendants regarding the same Replay Session Code; the allegations present unique expert discovery issues; and there is a risk of inconsistent rulings. The Actions are sufficiently numerous and complex to warrant consolidation.

II. The Western District of Washington Is The Most Appropriate Transferee Forum.

There is a significant nexus to the Western District of Washington and the Panel should transfer the Actions there. A significant “nexus” exists when a party which is common to all actions (*e.g.*, the defendant) is headquartered or has facilities that are located within the transferee court’s jurisdiction, such that relevant witnesses and documentary evidence common to all the

actions are likely to be found there. *In re FedLoan Student Loan Servicing Litig.*, 340 F. Supp. 3d 1377, 1378 (J.P.M.L. 2018) (transferring cases to a district “near defendant’s headquarters . . . where witnesses and documents [were] likely to be located”); *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 325 F. Supp. 3d 1362, 1364 (J.P.M.L. 2018) (transferring cases to the Northern District of California because it is “where Facebook is headquartered and relevant evidence and witnesses are likely to be located”); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 289 F. Supp. 3d 1322, 1326 (J.P.M.L. 2017) (transferring 97 cases to the Northern District of Georgia because “Equifax is headquartered in that district, and relevant documents and witnesses thus likely will be found there”); *In re Bair Hugger Forced Air Warming Devices Prods. Liab. Litig.*, 148 F. Supp. 3d 1383, 1386 (J.P.M.L. 2015) (transferring cases to the District of Minnesota because “defendants are headquartered in Minnesota, and many witnesses and relevant documents are likely to be found there.”); *In re Packaged Seafood Prods. Antitrust Litig.*, 148 F. Supp. 3d 1375, 1377 (J.P.M.L. 2015) (transferring cases to defendant’s home district because “relevant documents and witnesses are likely to be found there”); *In re Bard IVC Filters Prods. Liab. Litig.*, 122 F. Supp. 3d 1375, 1376-77 (J.P.M.L. 2015) (transferring to District of Arizona, where defendant was headquartered and documents and witnesses were there); *In re Lenovo Adware Litig.*, 109 F. Supp. 3d 1366, 1367 (J.P.M.L. 2015) (same); *In re Toyota Motor Corp. Hybrid Brake Mktg., Sales Practices, & Prod. Liab. Litig.*, 732 F. Supp. 2d 1375, 1377 (J.P.M.L. 2010) (“We are persuaded that the Central District of California is an appropriate transferee forum for this litigation. Defendants maintain their United States corporate headquarters within this district, and relevant documents and witnesses are likely located there.”).

The Western District of Washington is the center of gravity for the Actions: it is where Zillow (and Microsoft) are headquartered; where many of the witnesses are likely located; where

substantial acts regarding the alleged conduct occurred; and it is the venue agreed to by all users when they visit the website. *See* <https://www.zillowgroup.com/terms-of-use>. The Western District of Washington will serve the convenience of the parties and witnesses, and it will promote the just and efficient management of this litigation. It is the most appropriate transferee court.

CONCLUSION

For all the foregoing reasons, Zillow respectfully requests that the Panel enter an order consolidating for pretrial proceedings the putative class Actions already filed, as well as any other related actions that are subsequently filed, to the United States District Court for the Western District of Washington.

Dated: October 19, 2022

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

By: /s/ Samantha L. Southall

Samantha L. Southall
Two Liberty Place
50 S. 16th Street, Suite 3200
Philadelphia, Pennsylvania 19102
(215) 665-8700
samantha.southall@bipc.com

Christopher J. Dalton
550 Broad Street, Suite 810
Newark, New Jersey 07102-4582
(973) 273-9800
christopher.dalton@bipc.com

Jennifer Olmedo-Rodriguez
One Biscayne Tower
2 S. Biscayne Blvd., Suite 1500
Miami, Florida 33131
(305) 347-5900
jennifer.olmedo-rodriguez@bipc.com

Counsel for Zillow Group, Inc.

**BEFORE THE
UNITED STATES JUDICIAL PANEL
ON MULTIDISTRICT LITIGATION**

**In re: ZILLOW GROUP, INC. SESSION
REPLAY SOFTWARE LITIGATION**

MDL-__

SCHEDULE OF ACTIONS

	Case Caption	Court	Civil Action No.	Judge
1.	Plaintiff: Jamie Huber Defendant: Zillow Group, Inc.	United States District Court for the Eastern District of Pennsylvania	22-cv-03572	The Honorable Gerald J. Pappert
2.	Plaintiff: Ryan Margulis Defendant: Zillow Group, Inc.	United States District Court for the Northern District of Illinois	22-cv-04847	The Honorable Edmond E. Chang
3.	Plaintiff: Ashley Popa Defendant: Zillow Group, Inc.	United States District Court for the Western District of Pennsylvania	22-cv-01287	The Honorable William S. Stickman, IV
4.	Plaintiffs: Natalie Perkins and Kenneth Hasson Defendants: Zillow Group, Inc. and Microsoft Corporation	United States District Court for the Western District of Washington	22-cv-01282	The Honorable S. Kate Vaughan
5.	Plaintiff: David Kauffman Defendant: Zillow Group, Inc.	United States District Court for the Southern District of California	22-cv-01398	The Honorable Linda Lopez
6.	Plaintiff: Jill Strelzin Defendant: Zillow Group, Inc.	United States District Court for the Northern District of Illinois	22-cv-05644	The Honorable Steven C. Seeger

	Case Caption	Court	Civil Action No.	Judge
7.	Plaintiffs: Mark Conlisk and Michael Dekhtyar Defendant: Zillow Group, Inc.	United States District Court for the Northern District of Illinois	22-cv-05082	The Honorable John F. Kness
8.	Plaintiffs: Jill Adams Jill Adams as Natural Mother and Next Friend of her minor child, H.A. Defendant: Zillow Group, Inc.	United States District Court for the Eastern District of Missouri	22-cv-01023	The Honorable Shirley Padmore Mensah

Dated: October 19, 2022

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

By: /s/ Samantha L. Southall

Samantha L. Southall
Two Liberty Place
50 S. 16th Street, Suite 3200
Philadelphia, Pennsylvania 19102
(215) 665-8700
samantha.southall@bipc.com

Christopher J. Dalton
550 Broad Street, Suite 810
Newark, New Jersey 07102-4582
(973) 273-9800
christopher.dalton@bipc.com

Jennifer Olmedo-Rodriguez
One Biscayne Tower
2 S. Biscayne Blvd., Suite 1500
Miami, Florida 33131
(305) 347-5900
jennifer.olmedo-rodriguez@bipc.com

Counsel for Zillow Group, Inc.

**BEFORE THE
UNITED STATES JUDICIAL PANEL
ON MULTIDISTRICT LITIGATION**

**In re: ZILLOW GROUP, INC. SESSION
REPLAY SOFTWARE LITIGATION**

MDL-__

PROOF OF SERVICE

Pursuant to JPML Rule 4.1(a), I certify that the foregoing documents were served via e-mail and regular US mail on the following:

Ari H. Marcus, Esquire
MARCUS & ZELMAN LLC
701 Cookman Avenue, Suite 300
Asbury Park, NJ 07712
ari@marcuszelman.com
*Counsel for Plaintiff Jamie Huber and the
Putative Class*

Douglas A. Millen, Esquire
Michael E. Moskovitz, Esquire
FREED KANNER LONDON
& MILLEN LLC
2201 Waukegan Road, Ste. 130
Bannockburn, IL 60015
(224) 632-4500
dmillen@fkmlaw.com
mmoskovitz@fkmlaw.com
*Counsel for Ryan Margulis and the Putative
Class*

Gary Lynch, Esquire
Kelly K. Iverson, Esquire
Jamisen A. Etzel, Esquire
Elizabeth Pollock-Avery, Esquire
Nicholas A. Colella, Esquire
Patrick D. Donathen, Esquire
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
gary@lcllp.com
kelly@lcllp.com
jamisen@lcllp.com
elizabeth@lcllp.com
nickc@lcllp.com
patrick@lcllp.com
*Counsel for Plaintiff Ashley Popa and the
Putative Class*
*Counsel for Jill Strelzin and the Putative
Class*
*Counsel for Plaintiffs, Natalie Perkins and
Kenneth Hasson, and the Putative Class*

Jonathan M. Jagher, Esquire
FREED KANNER LONDON
& MILLEN LLC
923 Fayette Street
Conshohocken, Pennsylvania 19428
jjagher@fkmlaw.com
*Counsel for Ryan Margulis and the Putative
Class*

Katrina Carroll, Esquire
Kyle Shamberg, Esquire
LYNCH CARPENTER LLP
111 W. Washington Street, Suite 1240
Chicago, IL 60602
katrina@lcllp.com
kyle@lcllp.com
*Counsel for Plaintiff Jill Strelzin and the
Putative Class*

Joshua B. Swigart, Esquire
SWIGART LAW GROUP, APC
2221 Camino del Rio S., Suite 308
San Diego, CA 92108
Josh@SwigartLawGroup.com
*Counsel for Plaintiff David Kauffman and the
Putative Class*

Daniel G. Shay, Esquire
LAW OFFICE OF DANIEL G. SHAY
2221 Camino del Rio S., Suite 308
San Diego, CA 92108
DanielShay@TCPAFDCPA.com
*Counsel for Plaintiff David Kauffman and the
Putative Class*

Gary M. Klinger, Esquire
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
gklinger@milberg.com
*Counsel for Plaintiffs, Mary Conlisk and
Michael Dekhtyar, and the Putative Class*

Nick Suciu III
MILBERG COLEMAN BRYSON PHILLIPS
GROSSMAN, PLLC
6905 Telegraph Road, Suite 115
Bloomfield Hills, MI 48301
nsuciu@milberg.com
*Counsel for Plaintiffs, Mary Conlisk and
Michael Dekhtyar, and the Putative Class*

Kim D. Stephens, P.S., Esquire
Jason T. Dennett, Esquire
Kaleigh N. Boyd, Esquire
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
kstephens@tousley.com
jdennett@tousley.com
kboyd@tousley.com
*Counsel for Plaintiffs, Natalie Perkins and
Kenneth Hasson, and the Putative Class*

E. Kirk Wood, Esquire
Sharika Robinson, Esquire
Marcela Jenkins, Esquire
WOOD LAW FIRM, LLC
P. O. Box 382434
Birmingham, AL 35238-2434
kirk@woodlawfirmllc.com
*Counsel for Plaintiffs, Natalie Perkins and
Kenneth Hasson, and the Putative Class*

Joseph P. Guglielmo, Esquire
Carey Alexander, Esquire
Ethan Binder, Esquire
SCOTT+SCOTT ATTORNEYS
AT LAW LLP
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169
jguglielmo@scott-scott.com
calexander@scott-scott.com
ebinder@scott-scott.com

*Counsel for Plaintiffs, Natalie Perkins and
Kenneth Hasson, and the Putative Class*

James G. Snell, Esquire
PERKINS COIE LLP
3150 Porter Drive
Palo Alto, California 94304
JSnell@perkinscoie.com
Counsel for Microsoft Corporation

Tiffany Marko Yiatras, Esquire
CONSUMER PROTECTION LEGAL, LLC
308 Hutchinson Road
Ellisville, Missouri 63011-2029
tiffany@consumerprotectionlegal.com
*Counsel for Plaintiff Jill Adams and the
Putative Class*

Nicola Menaldo, Esquire
Anna M. Thompson, Esquire
PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101
NMenaldo@perkinscoie.com
AnnaThompson@perkinscoie.com
Counsel for Microsoft Corporation

Charles B. Casper, Esquire
MONTGOMERY MCCracken WALKER
& RHOADS LLP
1735 Market Street, 21st Floor
Philadelphia, PA 19103
ccasper@mmwr.com
Counsel for Microsoft Corporation

Bryan L. Bleichner, Esquire
CHESTNUT CAMBRONNE PA
100 Washington Avenue S, Suite 1700
Minneapolis, MN 55401
bbleichner@chestnutcambronne.com
*Counsel for Plaintiff Jill Adams and the
Putative Class*

Kate M. Baxter-Kauf, Esquire
Karen Hanson Riebel, Esquire
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
kmbaxter-kauf@locklaw.com
khriebel@locklaw.com
*Counsel for Plaintiff Jill Adams and the
Putative Class*

/s/ Samantha L. Southall
Samantha L. Southall

Dated: October 19, 2022

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA**

JAMIE HUBER, *individually and
on behalf of all others similarly situated,*

Plaintiff,

v.

ZILLOW GROUP, INC.,

Defendant.

Case No.

CLASS ACTION

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Jamie Huber brings this class action against Defendant Zillow Group, Inc. and alleges as follows upon personal knowledge as to Plaintiff and Plaintiff's own acts and experiences, and, as to all other matters, upon information and belief, including investigation on conducted by Plaintiff's attorneys.

NATURE OF THE ACTION

1. "Since the advent of online behavioral advertising ('OBA') in the late 1990s, businesses have become increasingly adept at tracking users visiting their websites." *Popa v. Harriet Carter Gifts, Inc.*, 426 F. Supp. 3d 108, 111 (W.D. Pa. 2019) (citations omitted). This case involves one of the most egregious examples of such consumer tracking and Internet privacy violations.

2. Plaintiff brings this case as a class action under the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Cons. Stat. 5701, *et seq.* ("WESCA"). The case stems from Defendant's unlawful interception of Plaintiff's and Class members' electronic

communications through the use of “session replay” spyware that allowed Defendant to watch and record Plaintiff’s and the Class members’ visits to its website.

3. As discussed in detail below, Defendant utilized “session replay” spyware to intercept Plaintiff’s and the Class members’ electronic computer-to-computer data communications with Defendant’s website, including how they interacted with the website, their mouse movements and clicks, keystrokes, search terms, information inputted into the website, and pages and content viewed while visiting the website. Defendant intercepted, stored, and recorded electronic communications regarding the webpages visited by Plaintiff and the Class members, as well as everything Plaintiff and the Class members did on those pages, *e.g.*, what they searched for, what they looked at, the information they inputted, and what they clicked on.

4. Defendant intercepted the electronic communications at issue without the knowledge or prior consent of Plaintiff or the Class members. Defendant did so for its own financial gain and in violation of Plaintiff’s and the Class members’ substantive legal privacy rights under the WESCA.

5. The “session replay” spyware utilized by Defendant is not a traditional website cookie, tag, web beacon, or analytics tool. It is a sophisticated computer software that allows Defendant to contemporaneously intercept, capture, read, observe, re-route, forward, redirect, and receive incoming electronic communications to its website. Plaintiff’s and the Class members’ electronic communications are then stored by Defendant using an outside vendor’s services and can later be viewed and utilized by Defendant to create a session replay, which is essentially a video of a Class member’s entire visit to Defendant’s website.

6. “Technological advances[.]” such as Defendant’s use of session replay technology, “provide ‘access to a category of information otherwise unknowable’ and ‘implicate privacy

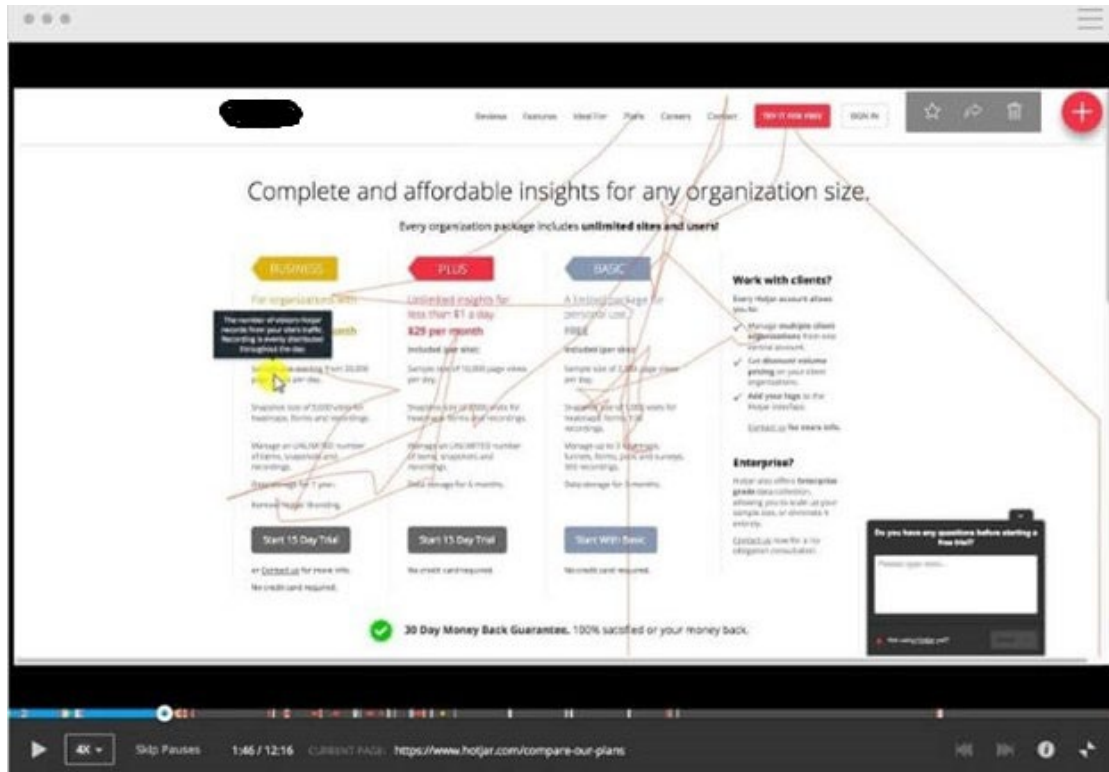
concerns’ in a manner different from traditional intrusions as a ‘ride on horseback’ is different from ‘a flight to the moon.’” *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1273 (9th Cir. 2019) (quoting *Riley v. California*, 573 U.S. 373, 393 (2014)).

7. The CEO of a major “session replay” software company – while discussing the merger of his company with another “session replay” provider – publicly exposed why companies like Defendant engage in recording visitors to their websites: “The combination of Clicktale and Contentsquare heralds an ***unprecedented goldmine of digital data*** that enables companies to interpret and predict the impact of any digital element -- including user experience, content, price, reviews and product -- on visitor behavior[.]” *See Contentsquare Acquires Clicktale to Create the Definite Global Leader in Experience Analytics*, available at www.prnewswire.com/news-releases/contentsquare-acquires-clicktale-to-create-the-definitive-global-leader-in-experience-analytics-300878232.html (last accessed May 10, 2021) (emphasis supplied). This CEO further admitted that “this unique data can be used to activate custom digital experiences in the moment via an ecosystem of over 50 martech partners. With a global community of customers and partners, ***we are accelerating the interpretation of human behavior online and shaping a future of addictive customer experiences.***” *Id.* (emphasis supplied).

8. Unlike typical website analytics services that provide aggregate statistics, the session replay technology utilized by Defendant is intended to record and playback individual browsing sessions, as if someone is looking over a Class members’ shoulder when visiting Defendant’s website. The technology also permits companies like Defendant to view the interactions of visitors on their website in live in real-time.

9. The following screenshots provide an example of a typical recording of a visit to a website captured utilizing session replay software, which includes mouse movements, keystrokes and clicks, search terms, content viewed, and information inputted by the website visitor:

Mouse Movements, Keystrokes, and Clicks:



Information Inputted During Live Website Session:

The left screenshot, labeled 'LIVE WEBSITE', shows a user profile form for 'John Doe'. The form includes sections for Employment (Company: Multi-Systems Merchant Services, Occupation: Sales engineer), Physical characteristics (Height: 5' 9" (174 centimeters), Weight: 204.8 pounds (93.1 kilograms), Blood type: A+), Contact Info (Name: John, Email: john@example.com, Phone: 16095550100), Shipping (Address: 123 Not a real street, City: New York, State: NY, Zip: 10001, Country: USA), Personal (Mother's maiden name: Doe, SSN: 078-05-1120, Birthday: 01/01/1980, Username: jdoe, Password: [REDACTED], Website: example.com), and Payment (Name on card: John Doe, Card Number: 4012 8888 8888 1881, Card Number Last Four: 1881, CVC: Empty).

The right screenshot, labeled 'SESSION REPLAY DASHBOARD', shows a list of events for 'User 15'. The events include 'Clicked', 'Changed ("T")', 'Changed ("B")', and 'Clicked'. The dashboard also shows a 'NEXT SESSION' section with a play button and a 'User 15' profile card.

LIVE WEBSITE

SESSION REPLAY DASHBOARD

10. The purported use of session replay technology is to monitor and discover broken website features. However, the extent and detail of the data collected by users of the technology, including Defendant, far exceeds the stated purpose and Plaintiff's and the Class members' expectations when visiting websites like Defendant's. The technology not only allows the recording and viewing of a visitor's electronic communications with a website, but also allows the user to create a detailed profile for each visitor to the site. Indeed, in an ongoing patent dispute, a well-known session replay provider openly admitted that this type of technology is utilized by companies like Defendant to make a profit: “[the] software computes billions of touch and mouse movements and transforms this knowledge into profitable actions that increase engagement, reduce operational costs, and maximize conversion rates (i.e., the percentage of users who take desired actions on a website, such as purchasing a product offered for sale).” *Content Square SAS v. Quantum Metric, Inc.*, Case No. 1:20-cv-00832-LPS, Compl. at ¶8, [DE 1] (D. Del. Jun. 22, 2020) (emphasis supplied).

11. Moreover, the collection and storage of page content may cause sensitive information and other personal information displayed on a page to leak to third parties. This may expose website visitors to identity theft, online scams, and other unwanted behavior.

12. In 2019, Apple warned application developers using session replay technology that they were required to disclose such tracking and recording to their users, or face being immediately removed from the Apple Store: “Protecting user privacy is paramount in the Apple ecosystem. Our App Store Review Guidelines require that apps request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity.” <https://techcrunch.com/2019/02/07/apple-glassbox-apps/> (last visited Mar. 16, 2021).

13. Consistent with Apple’s concerns, countless articles have been written about the privacy implications of recording user interactions during a visit to a website, including the following examples:

- (a) *The Dark Side of ‘Replay Sessions’ That Record Your Every Move Online*, located at <https://www.wired.com/story/the-dark-side-of-replay-sessions-that-record-your-every-move-online/> (last visited Mar. 16, 2021);
- (b) *Session-Replay Scripts Disrupt Online Privacy in a Big Way*, located at <https://www.techrepublic.com/article/session-replay-scripts-are-disrupting-online-privacy-in-a-big-way/> (last visited Mar. 16, 2021);
- (c) *Are Session Recording Tools a Risk to Internet Privacy?*, located at <https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/> (last visited Mar. 16, 2021);

(d) *Session Replay is a Major Threat to Privacy on the Web*, located at <https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720> (last visited Mar. 16, 2021);

(e) *Session Replay Scripts Could be Leaking Sensitive Data*, located at <https://medium.com/searchencrypt/session-replay-scripts-could-be-leaking-sensitive-data-5433364b2161> (last visited Mar. 16, 2021); and

(f) *Website Owners can Monitor Your Every Scroll and Click*, located at <https://www.digitalinformationworld.com/2020/02/top-brands-and-websites-can-monitor-your-every-scroll-and-click.html> (last visited Mar. 16, 2021).

14. In sum, Defendant intercepted the electronic communications of Plaintiff and the Class members through their visits to its website, causing them injuries, including violations of their substantive legal privacy rights under the WESCA, invasion of their privacy, and potential exposure of their private information.

15. Through this action, Plaintiff seeks damages authorized by the WESCA on behalf of herself and the Class members, defined below, and any other available legal or equitable remedies to which they are entitled.

PARTIES

16. Plaintiff is, and at all times relevant hereto was, a natural person and a permanent resident of the State of Pennsylvania.

17. Defendant is, and at all times relevant hereto was, a corporation duly organized and validly existing under the laws of Washington and maintains its principal place of business in Washington. Defendant is therefore a citizen of Washington.

JURISDICTION AND VENUE

18. This Court has personal jurisdiction over Defendant because Defendant directs, markets, and provides its business activities throughout the State of Pennsylvania, and makes its active commercial website available to residents of Pennsylvania for those interested in entering into contracts over the Internet with Defendant. Indeed, Defendant's website allows residents of Pennsylvania to make purchases utilizing the website. During the relevant time frame, Defendant entered into contracts for the sale of goods with residents of Pennsylvania that involved the knowing and repeated transmission of computer data over the Internet. This resulted in Defendant generating revenue from sales to residents of Pennsylvania, as well accepting payments from Pennsylvania residents through the site and ultimately shipping products to Pennsylvania. Plaintiff's and the Class members' claims arise directly from Defendant's operation of its website.

19. Further, this Court has personal jurisdiction over Defendant because Defendant's tortious conduct against Plaintiff occurred in substantial part within this District and because Defendant committed the same wrongful acts to other individuals within this judicial District, such that Defendant's acts complained of herein occurred within this District, subjecting Defendant to jurisdiction here. Thus, Defendant knew or should have known that it was causing harm to those individuals while they were in Pennsylvania such that it was foreseeable to Defendant that its interceptions would harm Plaintiff and other similarly-situated individuals located in Pennsylvania.

20. This court has subject matter jurisdiction under 28 U.S.C. § 1332(d)(2) because at least one member of the putative class, including Plaintiff, is a citizen of Pennsylvania, and Defendant is a citizen of Washington, thus CAFA's minimal diversity requirement is met. Additionally, Plaintiff seeks, at minimum, \$1,000.00 in damages for each violation, which, when

aggregated among a proposed class of over 5,000, exceeds the \$5,000,000 threshold for federal court jurisdiction under the Class Action Fairness Act (“CAFA”).

21. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b) and (c) because Defendant is deemed to reside in any judicial district in which it is subject to personal jurisdiction, and because a substantial part of the events or omissions giving rise to the claim occurred in this District, and because Plaintiff was injured in this District.

FACTS

22. Defendant owns and operates the following website: www.zillow.com.

23. Over the past year, Plaintiff visited Defendant’s website almost daily.

24. Plaintiff most recently visited Defendant’s website on or about September 2, 2022.

25. Plaintiff was in Pennsylvania during each visit to Defendant’s website.

26. During her visits to the website, Plaintiff, through her computer and/or mobile device, transmitted electronic communications in the form of instructions to Defendant’s computer servers utilized to operate the website. The commands were sent as messages instructing Defendant what content was being viewed, clicked on, requested and/or inputted by Plaintiff. The communications sent by Plaintiff to Defendant’s servers included, but were not limited to, the following actions taken by Plaintiff while on the website: mouse clicks and movements, keystrokes, search terms, information inputted by Plaintiff, pages and content viewed by Plaintiff, scroll movements, and copy and paste actions.

27. Defendant responded to Plaintiff’s electronic communications by supplying – through its website – the information requested by Plaintiff. *See Revitch v. New Moosejaw, LLC*, No. 18-cv-06827-VC, 2019 U.S. Dist. LEXIS 186955, at *3 (N.D. Cal. Oct. 23, 2019) (“This series of requests and responses — whether online or over the phone — is communication.”).

28. Plaintiff reasonably expected that her visits to Defendant’s website would be private and that Defendant would not be tracking, recording, and/or watching Plaintiff as she browsed and interacted with the website, particularly because Plaintiff was never presented with any type of pop-up disclosure or consent form alerting Plaintiff that her visits to the website were being recorded by Defendant.

29. Plaintiff reasonably believed that she was interacting privately with Defendant’s website, and not that she was being recorded and that those recordings could later be watched by Defendant’s employees, or worse yet, live while Plaintiff was on the website.

30. Upon information and belief, over at least the past two years, Defendant has had embedded within its website code and has continuously operated at least one session replay script¹ that was provided by a third party (a “Session Replay Provider”). The session replay spyware was always active and intercepted every incoming data communication to Defendant’s website the moment a visitor accessed the site.

31. The Session Replay Provider(s) that provided the session replay spyware to Defendant is not a provider of wire or electronic communication services, or an internet service provider.

32. Defendant is not a provider of wire or electronic communication services, or an internet service provider.

33. Defendant’s use of session replay spyware was not instrumental or necessary to the operation or function of Defendant’s website or business.

34. Defendant’s use of a session replay spyware to intercept Plaintiff’s electronic communications was not instrumental or necessary to Defendant’s provision of any of its goods

¹ A script is a sequence of computer software instructions.

or services. Rather, the level and detail of information surreptitiously collected by Defendant indicates that the only purpose was to gain an unlawful understanding of the habits and preferences of users to its website, and the information collected was solely for Defendant's own benefit.

35. Defendant's use of a session replay spyware to intercept Plaintiff's electronic communications did not facilitate, was not instrumental, and was not incidental to the transmission of Plaintiff's electronic communications with Defendant's website.

36. Upon information and belief, during one or more of Plaintiff's visits to Defendant's website, Defendant utilized session replay spyware to intentionally and contemporaneously intercept the substance of Plaintiff's electronic communications with Defendant's website, including mouse clicks and movements, keystrokes, search terms, information inputted by Plaintiff, pages and content viewed by Plaintiff, and scroll movements, and copy and paste actions. In other words, Defendant intercepted, stored, and recorded the webpages visited by Plaintiff, as well as everything Plaintiff did on those pages, what Plaintiff searched for, what Plaintiff looked at, and the information Plaintiff inputted.

37. The session replay spyware intentionally utilized by Defendant contemporaneously intercepted the electronic computer-to-computer data communications between Plaintiff's computer and/or mobile device and the computer servers and hardware utilized by Defendant to operate its website – as the communications were transmitted from Plaintiff's computer and/or mobile device to Defendant's computer servers and hardware – and copied and sent and/or re-routed the communications to a storage file within the Session Replay Provider(s)'s server(s). The intercepted data was transmitted contemporaneously to the Session Replay Provider(s) server(s) as it was sent from Plaintiff's computer and/or mobile device.

38. The relevant facts regarding the full parameters of the communications intercepted and how the interception occurred are solely within the possession and control of Defendant.

39. The session replay spyware utilized by Defendant is not a website cookie, standard analytics tool, tag, web beacon, or other similar technology.

40. Unlike the harmless collection of an internet protocol address, the data collected by Defendant identified specific information inputted and content viewed, and thus revealed personalized and sensitive information about Plaintiff's internet activity and habits.

41. The electronic communications intentionally intercepted by Defendant by Defendant was content generated through Plaintiff's intended use, interaction, and communication with Defendant's website relating to the substance, purport, and/or meaning of Plaintiff's communications with the website, *i.e.*, mouse clicks and movements, keystrokes, search terms, information inputted by Plaintiff, and pages and content clicked on and viewed by Plaintiff.

42. The electronic communications intentionally intercepted by Defendant were not generated automatically and were not incidental to Plaintiff's communications.

43. The session replay spyware utilized by Defendant intercepted, copied, replicated, and sent the data in a manner that was undetectable by Plaintiff.

44. Plaintiff's electronic data communications were then stored by Defendant and/or the Session Replay Provider(s).

45. The electronic data communications were not only intercepted and stored, but could also be used by Defendant to create a video playback of Plaintiff's visit to the website. Additionally, the session replay technology utilized by Defendant gave Defendant the ability to view Plaintiff's website visits live in real-time as they were occurring.

46. Defendant's interception of Plaintiff's electronic communications allowed Defendant to capture, observe, and divulge Plaintiff's personal interests, browsing history, queries, and habits as she interacted with and browsed Defendant's website.

47. Upon information and belief, Defendant similarly intercepted the electronic communications of at least 5,000 individuals located in Pennsylvania who visited Defendant's website.

48. Defendant utilized a spyware embedded within its website to intercept the communications at issue.

49. Defendant never alerted or asked Plaintiff or the Class Members for permission to intercept and record their visits to Defendant's website using "session replay" spyware.

50. Plaintiff and the Class members never consented to interception of their electronic communications by Defendant or anyone acting on Defendant's behalf, and they were never given the option to opt out of Defendant's recording.

51. At no point in time did Plaintiff or the Class members provide Defendant, its employees, or agents with consent to intercept their electronic communications using "session replay" spyware.

52. At no point in time did Plaintiff or the Class members specifically, clearly, and unmistakably consent to Defendant's interception and recording of their electronic communications using "session replay" spyware.

53. At no point in time did Plaintiff or the Class members specifically, clearly, and unmistakably consent to Defendant's interception and recording of their visits to Defendant's website using "session replay" spyware.

54. Plaintiff and the Class members did not have a reasonable opportunity to discover Defendant’s unlawful interceptions because Defendant did not disclose its interception nor seek consent from Plaintiff and the Class members prior to interception of their communications.

55. Plaintiff and the Class members never clicked or otherwise agreed to any disclosure or consent form authorizing Defendant to intercept Plaintiff’s and the Class members’ electronic communications using “session replay” spyware.

56. Defendant intercepted Plaintiff’s and the Class members’ electronic communications from the moment they landed on Defendant’s website, and before they had an opportunity to even consider consenting or agreeing to any privacy or terms of use policy on the website. In other words, Defendant’s unlawful interception occurred before Plaintiff and the Class members were given an opportunity to review, let alone consent, to any language that Defendant may claim purportedly authorized its violations of the WESCA.

57. Moreover, Defendant’s website failed to explicitly alert or otherwise notify Plaintiff and the Class members that Defendant would be utilizing session replay spyware to monitor and record their interactions with Defendant’s website.

58. Additionally, upon immediately landing on Defendant’s website, Plaintiff and the Class members were not alerted that by entering the website Defendant would unilaterally attempt to bind them Defendant’s terms and policies or privacy policy. Indeed, the landing page to Defendant’s website not only fails to advise visitors that Defendant is intercepting their electronic communications, it does not contain any type of conspicuous disclosure regarding Defendant’s terms of use or privacy policy.

59. Plaintiff and the Class members were not immediately required to click on any box or hyperlink containing Defendant's terms of use or privacy policy upon visiting the website or in order to navigate through the website.

60. Plaintiff and the Class members were not placed on notice of Defendant's terms and policies or privacy policy upon immediately visiting the website. Instead, Defendant's terms of use and privacy policy are buried at the bottom of Defendant's website where Plaintiff and the Class members were unable to see them.

61. Defendant does not require visitors to its website to immediately and directly acknowledge that the visitor has read Defendant's terms of use or privacy policy before proceeding to the site. In other words, Defendant's website does not immediately direct visitors to the site to the terms of use or privacy policy, and does not require visitors to click on a box to acknowledge that they have reviewed the terms and conditions/policy in order to proceed to the website.

62. Upon information and belief, at least one of the purposes of Defendant's interception of Plaintiff's and the Class members' electronic communications was to allow Defendant to learn of Plaintiff's and the Class members' personal preferences and likes, which would then be used to market Defendant's services and goods to Plaintiff and the Class members.

63. Defendant's surreptitious interception of Plaintiff's and the Class members' electronic communications caused Plaintiff and the Class members harm, including violations of their substantive legal privacy rights under the WESCA, invasion of privacy, invasion of their rights to control information concerning their person, and/or the exposure of their private information. Moreover, Defendant's practices caused harm and a material risk of harm to Plaintiff's and the Class Members' privacy and interest in controlling their personal information, habits, and preferences.

CLASS ALLEGATIONS

PROPOSED CLASS

64. Plaintiff brings this lawsuit as a class action on behalf of all other similarly situated persons pursuant to Federal Rule of Civil Procedure 23. The “Class” that Plaintiff seeks to represent is defined as:

All persons residing within the State of Pennsylvania (1) who visited Defendant’s website and (2) whose electronic communications were intercepted by Defendant or on Defendant’s behalf (3) without their prior consent.

65. Defendant and its employees or agents are excluded from the Class. Plaintiff reserves the right to modify or amend the Class definitions, as appropriate, during the course of this litigation.

NUMEROSITY

66. The Class members are so numerous that individual joinder of all Class members is impracticable. Upon information and belief, Defendant intercepted the electronic communications of over 5,000 individuals. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include notice on Defendant’s website, U.S. Mail, electronic mail, Internet postings, and/or published notice.

67. The identities of the Class members are unknown at this time and can be ascertained only through discovery. Identification of the Class members is a matter capable of ministerial determination from Defendant’s records kept in connection with its unlawful interceptions.

COMMON QUESTIONS OF LAW AND FACT

68. There are numerous questions of law and fact common to the Class which predominate over any questions affecting only individual members of the Class. Among the questions of law and fact common to the Class are:

- (1) Whether Defendant violated the WESCA;
- (2) Whether Defendant intercepted Plaintiff's and the Class members' electronic communications;
- (3) Whether Defendant disclosed to Plaintiff and the Class Members that it was intercepting their electronic communications;
- (4) Whether Defendant secured prior consent before intercepting Plaintiff's and the Class members' electronic communications; and
- (5) Whether Defendant is liable for damages, and the amount of such damages.

69. The common questions in this case are capable of having common answers. If Plaintiff's claim that Defendants routinely intercepts electronic communications without securing prior consent is accurate, Plaintiff and the Class members will have identical claims capable of being efficiently adjudicated and administered in this case.

TYPICALITY

70. Plaintiff's claims are typical of the claims of the Class members, as they are all based on the same factual and legal theories.

PROTECTING THE INTERESTS OF THE CLASS MEMBERS

71. Plaintiff is a representative who will fully and adequately assert and protect the interests of the Class and has retained competent counsel. Accordingly, Plaintiff is an adequate representative and will fairly and adequately protect the interests of the Class.

SUPERIORITY

72. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the claims of all members of the Class is economically unfeasible and procedurally impracticable. While the aggregate damages sustained

by the Class are potentially in the millions of dollars, the individual damages incurred by each member of the Class resulting from Defendant's wrongful conduct are too small to warrant the expense of individual lawsuits. The likelihood of individual Class members prosecuting their own separate claims is remote, and, even if every member of the Class could afford individual litigation, the court system would be unduly burdened by individual litigation of such cases.

73. The prosecution of separate actions by members of the Class would create a risk of establishing inconsistent rulings and/or incompatible standards of conduct for Defendant. For example, one court might enjoin Defendant from performing the challenged acts, whereas another may not. Additionally, individual actions may be dispositive of the interests of the Class, although certain class members are not parties to such actions.

COUNT I
Violations of the WESCA, 18 Pa. Cons. Stat. 5701, *et seq.*
(On Behalf of Plaintiff and the Class)

74. Plaintiff re-alleges and incorporates the foregoing allegations as if fully set forth herein.

75. The Pennsylvania Wiretap and Electronic Surveillance Control Act (the "Act") prohibits (1) the interception or procurement of another to intercept any wire, electronic, or oral communication; (2) the intentional disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication; and (3) the intentional use of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication. 18 Pa. Cons. Stat. § 5703.

76. Any person who intercepts, discloses, or uses or procures any other person to intercept, disclose, or use, a wire, electronic, or oral communication in violation of the Act is

subject to a civil action for (1) actual damages, not less than liquidated damages computed at the rate of \$100/day for each violation or \$1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred. 18 Pa. Cons. Stat. § 5725(a).

77. Defendant procured Session Replay software to automatically and secretly spy on, and intercept, Defendant's website visitor's electronic communications with Defendant in real-time.

78. To facilitate this wiretap, Defendant installed its Session Replay Provider's code on its website.

79. Upon information and belief, Defendant knew that its Session Replay Provider would add its visitor's information, procured through the wiretap, to its back-end database and disclose that information to other users of its Session Replay Provider's code as part of its effort to de-anonymize visitors.

80. Upon information and belief, Defendant intentionally used information of its visitors, obtained through its Session Replay Provider's wiretap on other websites, to de-anonymize users of Defendant's site.

81. Defendant intentionally intercepted Defendant's website visitors' electronic communications in real-time.

82. Plaintiff and the putative class members engaged in communications with Defendant through use of Defendant's website.

83. Plaintiff and the putative class members had a justified and reasonable expectation under the circumstances that their electronic communications would not be intercepted.

84. Defendant employed its Session Replay Provider to intercept Plaintiff and the putative class members' electronic communications with Defendant.

85. Because the code is secret and encrypted, Plaintiff and the putative class members were not aware that their electronic communications were being intercepted by Defendant's Session Replay Provider.

86. Plaintiff and the putative class members did not consent to having their communications intercepted by Defendant or its Session Replay Provider.

87. As a result of Defendant's conduct, and pursuant to § 5725 of the WESCA, Plaintiff and the other members of the putative Class were harmed and are each entitled to actual damages, liquidated damages, punitive damages, reasonable attorneys' fees and costs. 18 Pa. Cons. Stat § 5725(a).

WHEREFORE, Plaintiff, on behalf of herself and the other members of the Class, prays for the following relief:

- a. An order certifying the Class and appointing Plaintiff as Class Representative and her counsel as Class Counsel;
- b. An award of actual damages, statutory damages, liquidated damages, and/or punitive statutory damages;
- c. An aware of reasonable attorney's fees and costs; and
- d. Such further and other relief the Court deems reasonable and just.

JURY DEMAND

Plaintiff and Class Members hereby demand a trial by jury on all issues so triable.

DOCUMENT PRESERVATION DEMAND

Plaintiff demands that Defendant take affirmative steps to preserve all records, lists, electronic databases or other itemizations associated with the allegations herein, including all records, lists, electronic databases or other itemizations in the possession of any vendors,

individuals, and/or companies contracted, hired, or directed by Defendant to assist in sending the alleged communications.

Dated: September 7, 2022

Respectfully Submitted,

By: **MARCUS ZELMAN LLC**

/s/ Ari H. Marcus

Ari H. Marcus, Esq. (Pennsylvania Bar
No. 322283)

701 Cookman Avenue, Suite 300
Asbury Park, New Jersey 07712

Telephone: (732) 695-3282

Fascimile: (732) 298-6256

Ari@marcuszelman.com

Counsel for Plaintiff and Proposed Class

CERTIFICATION PURSUANT TO LOCAL RULE 11.2

I, Ari H. Marcus, the undersigned attorney of record for Plaintiff, do hereby certify to my own knowledge and based upon information available to me at my office, the matter in controversy is not the subject of any other action now pending in any court or in any arbitration or administrative proceeding.

Dated: September 7, 2022

/s/ Ari H. Marcus

Ari H. Marcus, Esq.

United States District Court
Eastern District of Pennsylvania (Philadelphia)
CIVIL DOCKET FOR CASE #: 2:22-cv-03572-GJP

HUBER v. ZILLOW GROUP, INC.
Assigned to: HONORABLE GERALD J. PAPPERT
Cause: 18:2511 Wiretapping

Date Filed: 09/07/2022
Jury Demand: Plaintiff
Nature of Suit: 890 Other Statutes: Other
Statutory Actions
Jurisdiction: Federal Question

Plaintiff

JAMIE HUBER
individually and on behalf of all others
similarly situated

represented by **ARI H. MARCUS**
MARCUS & ZELMAN LLC
701 COOKMAN AVENUE
SUITE 300
ASBURY PARK, NJ 07712
732-695-3282
Email: ari@marcuszelman.com
ATTORNEY TO BE NOTICED

V.

Defendant

ZILLOW GROUP, INC.

represented by **SAMANTHA L. SOUTHALL**
BUCHANAN INGERSOLL & ROONEY
PC
50 S. 16TH ST STE 3200
TWO LIBERTY PLACE
PHILADELPHIA, PA 19102
215-665-3884
Email: samantha.southall@bipc.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
09/07/2022	<u>1</u>	COMPLAINT against ZILLOW GROUP, INC. (Filing fee \$ 402 receipt number APAEDC-16156488.), filed by JAMIE HUBER. (Attachments: # <u>1</u> Civil Cover Sheet, # <u>2</u> Designation Form, # <u>3</u> Summons)(MARCUS, ARI) (Entered: 09/07/2022)
09/07/2022	<u>2</u>	Summons Issued as to ZILLOW GROUP, INC. Forwarded To: Counsel on 9/7/22 (er) (Entered: 09/09/2022)
09/15/2022	<u>3</u>	SUMMONS Returned Executed by JAMIE HUBER re: Isaac Espinoza served Summons and Complaint upon ZILLOW GROUP, INC. by Personal. ZILLOW GROUP, INC. served on 9/13/2022, answer due 10/4/2022. (MARCUS, ARI) (Entered: 09/15/2022)
09/29/2022	<u>4</u>	STIPULATION re <u>1</u> Complaint (Attorney) <i>to Extend Time to Answer or Otherwise Respond</i> by ZILLOW GROUP, INC.. (SOUTHALL, SAMANTHA) (Entered: 09/29/2022)
09/30/2022	<u>5</u>	STIPULATION TO EXTEND TIME FOR DEFENDANT ZILLOW GROUP, INC. TO ANSWER OR OTHERWISE RESPOND TO PLAINTIFFS COMPLAINT BY 11/3/2022.

SIGNED BY HONORABLE GERALD J. PAPPERT ON 9/30/22. 9/30/22 ENTERED
AND COPIES E-MAILED. (va) (Entered: 09/30/2022)

PACER Service Center			
Transaction Receipt			
10/19/2022 11:35:59			
PACER Login:	samanthasouthall	Client Code:	0106198-000001-SS
Description:	Docket Report	Search Criteria:	2:22-cv-03572-GJP
Billable Pages:	1	Cost:	0.10

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS**

RYAN MARGULIS, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

ZILLOW GROUP, INC.,

Defendant.

Case No. _____

JURY TRIAL DEMANDED

COMPLAINT - CLASS ACTION

Plaintiff Ryan Margulis (“Plaintiff”), individually and on behalf of all others similarly situated, hereby files this class action complaint against Defendant Zillow Group, Inc. (“Defendant” or “Zillow”), and in support thereof alleges the following:

INTRODUCTION

1. This is a class action brought against Zillow for surreptitiously intercepting the private electronic communications of visitors to its website, www.zillow.com, without their consent. Zillow knowingly directs third-party vendors, such as Microsoft Corporation, to embed snippets of JavaScript computer code (“Session Replay Code”) on Zillow’s website, which then deploys on each website visitor’s internet browser for the purpose intercepting and recording the website visitor’s private electronic communications with the Zillow website, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time (“Website Communications”). These third-party vendors (collectively, “Session Replay Providers”) create and deploy the Session Replay Code at Zillow’s request.

2. After intercepting and recording the Website Communications, Zillow and the Session Replay Providers use those Website Communications to recreate website visitors' entire visit to www.zillow.com. The Session Replay Providers create a video replay of the user's behavior on the website and provide it to Zillow for analysis. Zillow's directive to the Session Replay Providers to secretly deploy the Session Replay Code results in the electronic equivalent of "looking over the shoulder" of each visitor to the Zillow website for the entire duration of their website interaction.

3. Zillow's conduct violates the Illinois Eavesdropping Act, 720 ILCS 5/14-1, *et seq.*, the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.*, and constitutes an invasion of the privacy rights of website visitors.

4. Plaintiff brings this action individually and on behalf of a class of all Illinois citizens whose Website Communications were intercepted at Zillow's direction and use of Session Replay Code embedded on the webpages of www.zillow.com and seeks all civil remedies provided under the causes of action, including but not limited to compensatory, statutory, and/or punitive damages, and attorneys' fees and costs.

PARTIES

5. Plaintiff Ryan Margulis is a citizen of the state of Illinois, and at all times relevant to this action, resided and was domiciled in Cook county, Illinois. Plaintiff is a citizen of Illinois.

6. Defendant Zillow Group, Inc. is corporation organized under the laws of Washington, and its principal place of business is located at 1301 Second Ave., Floor 31, Seattle Washington, 98101. Defendant is a citizen of Washington.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of \$5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class, including Plaintiff, is a citizen of a state different than Defendant.

8. This Court has personal jurisdiction over Defendant because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in Illinois. The privacy violations complained of herein resulted from Defendant's purposeful and tortious acts directed towards citizens of Illinois while they were located within Illinois. At all relevant times, Defendant knew that its practices would directly result in collection of information from Illinois citizens while those citizens browse www.zillow.com. Defendant chose to avail itself of the business opportunities of making its real property and rental advertising services specifically available in Illinois (and specifically with respect to Illinois properties) and collecting real-time data from website visit sessions initiated by Illinoisans while located in Illinois, and the claims alleged herein arise from those activities.

9. Zillow also knows that many users visit and interact with Zillow's websites while they are physically present in Illinois. Both desktop and mobile versions of Zillow's website allow a user to search for nearby properties by providing the user's "current location," as furnished by the location-determining tools of the device the user is using or by the user's IP address (*i.e.*, without requiring the user to manually input an address). Users' employment of automatic location services in this way means that Zillow is continuously made aware that its website is being visited

by people located in Illinois, and that such website visitors are being eavesdropped on in violation of Illinois statutory and common law.

10. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

FACTUAL ALLEGATIONS

A. Website User and Usage Data Have Immense Economic Value.

11. The “world’s most valuable resource is no longer oil, but data.”¹

12. Earlier this year, Business News Daily reported that some businesses collect personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data (*i.e.*, how consumers interact with a business’s website, applications, and emails), behavioral data (*i.e.*, customers’ purchase histories and product usage information), and attitudinal data (*i.e.*, data on consumer satisfaction) from consumers.² This information is valuable to companies because they can use this data to improve customer experiences, refine their marketing strategies, capture data to sell it, and even to secure more sensitive consumer data.³

13. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business’s success.

¹ *The world’s most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

² Max Freedman, *How Businesses Are Collecting Data (And What They’re Doing With It)*, Business News Daily (Aug. 5, 2022), <https://www.businessnewsdaily.com/10625-businesses-collecting-data.html>.

³ *Id.*

Research shows that organizations who “leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin.”⁴

14. In 2013, the Organization for Economic Cooperation and Development (“OECD”) even published a paper entitled “Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value.”⁵ In this paper, the OECD measured prices demanded by companies concerning user data derived from “various online data warehouses.”⁶

15. OECD indicated that “[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e. \$2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver’s license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55.”⁷

B. Website Users Have a Reasonable Expectation of Privacy in Their Interactions with Websites.

16. Consumers are skeptical and are wary about their data being collected. A report released by KPMG shows that “a full 86% of the respondents said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected.”⁸

⁴ Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), <https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data>.

⁵ Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), <https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf>.

⁶ *Id.* at 25.

⁷ *Id.*

⁸ Lance Whitney, *Data privacy is a growing concern for more consumers*, TechRepublic (Aug. 17, 2021), <https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/>.

17. Another recent paper also indicates that most website visitors will assume their detailed interactions with a website will only be used by the website and not be shared with a party they know nothing about.⁹ As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.¹⁰

18. Privacy polls and studies show that a majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

19. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.¹¹

20. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.¹²

21. Users act consistently with their expectation of privacy. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing

⁹ *CUJO AI Recent Survey Reveals U.S. Internet Users Expectations and Concerns Towards Privacy and Online Tracking*, CUJO (May 26, 2020), <https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html>.

¹⁰ Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, *The Information Society*, 38:4, 257, 258 (2022).

¹¹ *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, Consumer Reports (May 11, 2017), <https://www.consumerreports.org/consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/>.

¹² *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, (Nov. 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confusedand-feeling-lack-of-control-over-their-personal-information/>.

companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.¹³

C. How Session Replay Code Works.

22. Session Replay Code, such as that implemented on www.zillow.com, enables website operators to record, save, and replay website visitors' interactions with a given website. The clandestinely deployed code provides online marketers and website designers with insights into the user experience by recording website visitors "as they click, scroll, type or navigate across different web pages."¹⁴

23. While Session Replay Code is utilized by websites for some legitimate purposes, it goes well beyond normal website analytics when it comes to collecting the actual contents of communications between website visitors and websites. Unlike other online advertising tools, Session Replay Code allows a website to capture and record nearly every action a website visitor takes while visiting the website, including actions that reveal the visitor's personal or private sensitive data, sometimes even when the visitor does not intend to submit the data to the website operator, or has not finished submitting the data to the website operator.¹⁵ As a result, website visitors "aren't just sharing data with the [web]site they're on . . . but also with an analytics service that may be watching over their shoulder."¹⁶

¹³ Margaret Taylor, *How Apple screwed Facebook*, Wired, (May 19, 2021), <https://www.wired.co.uk/article/apple-ios14-facebook>.

¹⁴ Erin Gilliam Haije, *[Updated] Are Session Recording Tools a Risk to Internet Privacy?*, Mopinion (Mar. 7, 2018), <https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/>.

¹⁵ *Id.*

¹⁶ Eric Ravenscraft, *Almost Every Website You Visit Records Exactly How Your Mouse Moves*, Medium (Feb. 5, 2020), <https://onezero.medium.com/almost-every-website-you-visit-records-exactly-how-your-mouse-moves-4134cb1cc7a0>.

24. Session Replay Code works by inserting computer code into the various event handling routines that web browsers use to receive input from users, thus intercepting the occurrence of actions the user takes. When a website delivers Session Replay Code to a user's browser, the browser will follow the code's instructions by sending responses in the form of "event" data to a designated third-party server. Typically, the server receiving the event data is controlled by the third-party entity that wrote the Session Replay Code, rather than the owner of the website where the code is installed.

25. The types of events captured by Session Replay Code vary by specific product and configuration, but in general are wide-ranging and can encompass virtually every user action, including all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entry, and numerous other forms of a user's navigation and interaction through the website. In order to permit a reconstruction of a user's visit accurately, the Session Replay Code must be capable of capturing these events at hyper-frequent intervals, often just milliseconds apart. Events are typically accumulated and transmitted in blocks periodically throughout the user's website session, rather than after the user's visit to the website is completely finished.

26. Unless specifically masked through configurations chosen by the website owner, some visible contents of the website may also be transmitted to the Session Replay Provider.

27. Once the events from a user session have been recorded by a Session Replay Code, a website operator can view a visual reenactment of the user's visit through the Session Replay Provider, usually in the form of a video, meaning "[u]nlike typical analytics services that provide

aggregate statistics, these scripts are intended for the recording and playback of individual browsing sessions.”¹⁷

28. Because most Session Replay Codes will by default indiscriminately capture the maximum range of user-initiated events and content displayed by the website, researchers have found that a variety of highly sensitive information can be captured in event responses from website visitors, including medical conditions, credit card details, and other personal information displayed or entered on webpages.¹⁸

29. Most alarming, Session Replay Code may capture data that the user did not even intentionally transmit to a website during a visit, and then make that data available to website owners when they access the session replay through the Session Replay Provider. For example, if a user writes information into a text form field, but then chooses not to click a “submit” or “enter” button on the website, the Session Replay Code may nevertheless cause the non-submitted text to be sent to the designated event-response-receiving server before the user deletes the text or leaves the page. This information will then be viewable to the website owner when accessing the session replay through the Session Replay Provider.

30. Session Replay Code does not necessarily anonymize user sessions, either.

31. First, if a user’s entry of personally identifying information is captured in an event response, that data will become known and visible to both the Session Replay Provider and the website owner.

¹⁷ Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), <https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/>.

¹⁸ *Id.*

32. Second, if a website displays user account information to a logged-in user, that content may be captured by Session Replay Code.

33. Third, some Session Replay Providers explicitly offer website owners cookie functionality that permits linking a session to an identified user, who may be personally identified if the website owner has associated the user with an email address or username.¹⁹

34. Session Replay Providers often create “fingerprints” that are unique to a particular user’s combination of computer and browser settings, screen configuration, and other detectable information. The resulting fingerprint, which is often unique to a user and rarely changes, are collected across all sites that the Session Replay Provider monitors.

35. When a user eventually identifies themselves to one of these websites (such as by filling in a form), the provider can then associate the fingerprint with the user identity and can then back-reference all of that user’s other web browsing across other websites previously visited, including on websites where the user had intended to remain anonymous—even if the user explicitly indicated that they would like to remain anonymous by enabling private browsing.

36. In addition to the privacy invasions caused by the diversion of user communications with websites to third-party Session Replay Providers, Session Replay Code also exposes website visitors to identity theft, online scams, and other privacy threats.²⁰ Indeed, “[t]he more copies of sensitive information that exist, the broader the attack surface, and when data is being collected [

¹⁹ *Id.*; see also *FS.identify – Identifying users*, FullStory, <https://help.fullstory.com/hc/en-us/articles/360020828113>, (last visited Sep. 8, 2022).

²⁰ Juha Sarrinen, *Session Replay is a Major Threat to Privacy on the Web*, itnews (Nov. 16, 2017), <https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720>.

] it may not be stored properly or have standard protections” increasing “the overall risk that data will someday publicly leak or be breached.”²¹

37. Recognizing the privacy concerns posed by Session Replay Code, in 2019 Apple required app developers to remove or properly disclose the use of analytics code that allow app developers to record how a user interacts with their iPhone apps or face immediate removal from the app store.²² In announcing this decision, Apple stated: “Protecting user privacy is paramount in the Apple ecosystem. Our App Store Review Guidelines require that apps request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity.”²³

D. Zillow Secretly Eavesdrops on its Website Visitors’ Electronic Communications.

38. Zillow operates the website www.zillow.com. Zillow is the “leading online residential real estate” marketplace in the United States for consumers, connecting them to the information and real estate professionals they need to buy, sell, or rent a home.²⁴

39. Zillow has become “synonymous with residential real estate.”²⁵ www.zillow.com is the most popular real estate website in the United States, with over thirty-six million unique

²¹ Lily Hay Newman, *Covert ‘Replay Sessions’ Have Been harvesting Passwords by Mistake*, WIRED (Feb. 26, 2018), <https://www.wired.com/story/covert-replay-sessions-harvesting-passwords/>.

²² Zack Whittaker, *Apple Tells App Developers to Disclose or Remove Screen Recording Code*, TechCrunch (Feb. 7, 2019), <https://techcrunch.com/2019/02/07/apple-glassbox-apps/>.

²³ *Id.*

²⁴ Zillow Group, Inc., *Form 10-K* (Dec. 31, 2021), <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001617640/87bbbf30-39cb-4eb7-acdc-1b51265b9687.pdf> (“Zillow 10-K”).

²⁵ *Id.*

monthly visitors²⁶ and more than 135 million properties are listed on its website.²⁷ According to a 2021 Google Trends report, “[t]oday more people search ‘Zillow’ than ‘real estate.’”²⁸

40. However, unbeknownst to the millions of individuals perusing Zillow’s real estate listings, Zillow knowingly directs Session Replay Providers to embed various Session Replay Codes on its website to track and analyze website user interactions with www.zillow.com. Because the Session Replay Providers are unknown eavesdroppers to visitors to www.zillow.com, they are not parties to website visitors’ Website Communications with Zillow.

41. One such Session Replay Provider that Zillow procures is Microsoft.

42. Microsoft is the owner and operator of a Session Replay Code titled Clarity, which provides basic information about website user sessions, interactions, and engagement, and breaks down users by device type, county, and other dimensions.²⁹

43. Zillow knowingly derives a benefit and/or information from the Website Communications intercepted and recorded at its direction. Upon information and belief, Zillow uses the intercepted Website Communications to replay website visitors’ interactions with www.zillow.com, improve user interactions with its website, and to provide targeted real estate advertisements to its website visitors.

44. Zillow’s knowing direction and use of Microsoft Clarity’s Session Replay Code, direction and use of other Session Replay Codes through various Session Replay Providers, and its knowing derivation of a benefit and/or information from the Website Communications

²⁶ *Most Popular Real Estate Websites in the United States as of October 2021, Based on Unique Monthly Visits*, Statista, <https://www.statista.com/statistics/381468/most-popular-real-estate-websites-by-monthly-visits-usa/>, (last visited Sep. 8, 2022).

²⁷ Zillow 10-K, *supra*, note 1.

²⁸ *Id.*

²⁹ Jono Alderson, *An Introduction to Microsoft Clarity*, Yoast, <https://yoast.com/introduction-microsoft-clarity/#h-what-is-microsoft-clarity>, (last visited Sep. 8, 2022).

surreptitiously intercepted and recorded by Session Replay Codes is a violation of Illinois statutory and common law.

E. Plaintiff's and Class Members' Experience.

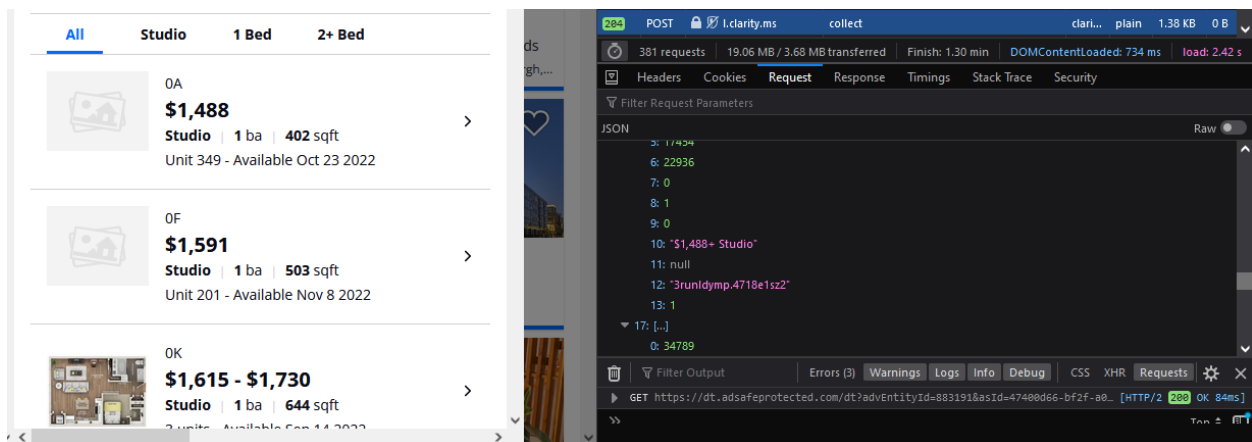
45. Plaintiff has visited www.zillow.com on his mobile devices and computer while in Illinois.

46. While visiting Zillow's website, Plaintiff fell victim to Defendant's unlawful monitoring, recording, and collection of Plaintiff's Website Communications with www.zillow.com.

47. Unknown to Plaintiff, Zillow directs Session Replay Providers to embed Session Replay Code on its website.

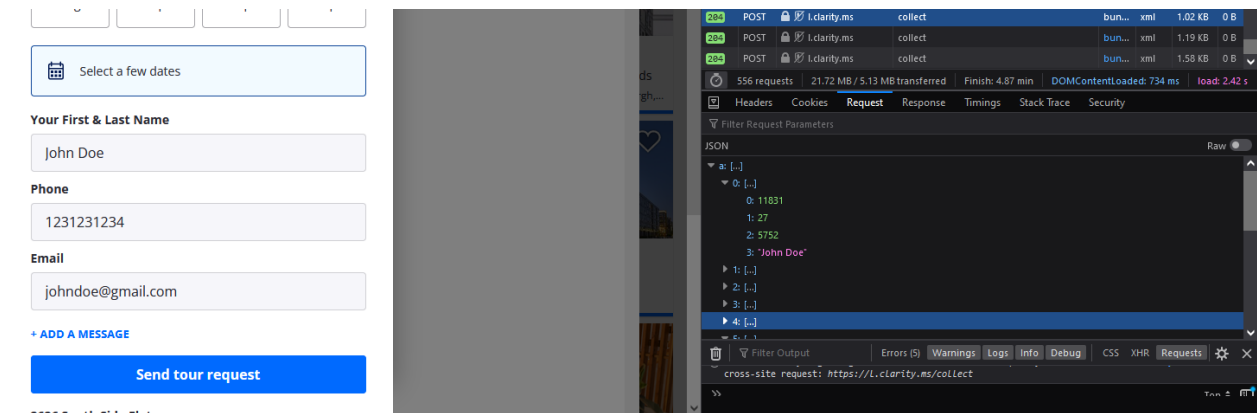
48. During the website visit, Plaintiff's Website Communications were captured by Session Replay Code and sent to various Session Replay Providers.

49. For example, when visiting www.zillow.com, if a website user views a certain piece of property for rent or sale, that information is captured by the Session Replay Codes embedded on the website:



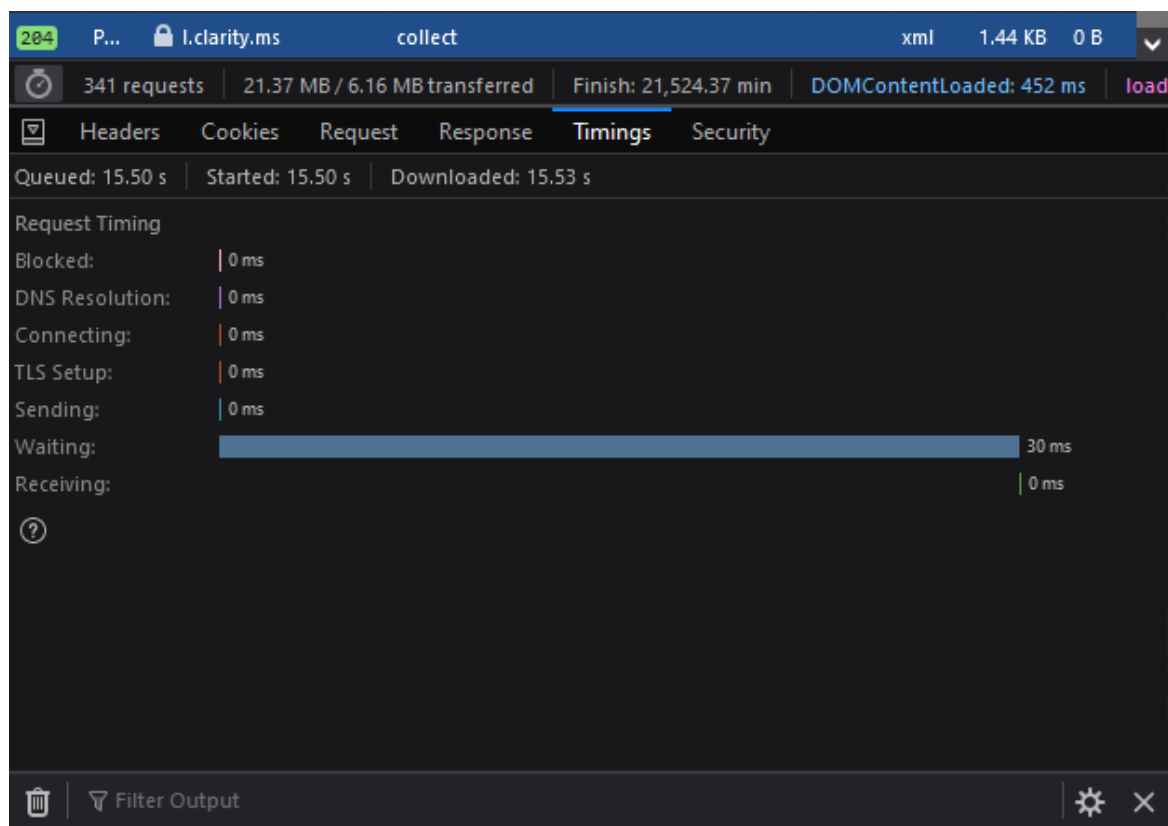
Depicting information sent to one of the Service Replay Providers—Microsoft—through a Service Replay Code—Clarity—after viewing a Studio apartment priced at \$1,488 while visiting www.zillow.com.

50. Similarly, when visiting www.zillow.com, if a user enters personal information in a text box to schedule a tour, that information is captured by the Session Replay Codes embedded on the website:



Depicting information sent to one of the Service Replay Providers—Microsoft—through a Service Replay Code—Clarity—after entering a name (purple text) to a text box to schedule a tour of a property.

51. The eavesdropping by the Session Replay Code is ongoing during the visit and they intercept the contents of these communications between Plaintiff and Zillow with instantaneous transmissions to the Session Replay Providers, as illustrated below, in which only 30 milliseconds were required to send a packet of even response data, which would indicate whatever the website user had just done:



52. The Session Replay Codes operate in the same manner for all putative Class members.

53. Like Plaintiff, each Class member visited www.zillow.com with Session Replay Code embedded in it, and those Session Replay Codes intercepted the Class members' Website Communications with www.zillow.com by sending hyper-frequent logs of those communications to Session Replay Providers.

54. Even if Zillow masks certain elements when it configures the settings of the Session Replay Code embedded on its website, any operational iteration of the Session Replay Code will, by its very nature and purpose, intercept the contents of communications between the website's visitors and the website owner.

55. For example, even with heightened masking enabled, Session Replay Providers will still learn through the intercepted data exactly which pages a user navigates to, how the user moves

through the page (such as which areas the user zooms in on or interacted with), and additional substantive information.

56. As a specific example, if a user types a particular address or zip code into Zillow's main search bar and initiates a search, even if the text entered into the search bar is masked, Session Replay Providers will still learn what is entered into the bar as soon as the search result page loads. This is so because the responsive search results will be displayed on the subsequent page, and the responsive content generated by Zillow will repeat the searched information back on the generated page. That information will not be masked even if user-inputted text is fully masked in a text field.

CLASS ACTION ALLEGATIONS

57. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Class:

All natural persons in the State of Illinois whose Website Communications were captured through the use of Session Replay Code embedded in www.zillow.com.

58. Excluded from the class are Defendant, its parents, subsidiaries, affiliates, officers, and directors, all persons who make a timely election to be excluded from the class, the judge to whom this case is assigned and any immediate family members thereof, and the attorneys who enter their appearance in this action.

59. **Numerosity:** The members of the Class are so numerous that individual joinder of all Class members is impracticable. The precise number of Class members and their identities may be obtained from the books and records of Zillow or the Session Replay Providers.

60. **Commonality:** This action involves questions of law and fact that are common to the Class members. Such common questions include, but are not limited to: (a) whether Defendant employed Session Replay Providers to intercept and record Zillow's website visitors' Website Communications; (b) whether Defendant operated or participated in the operation of an

eavesdropping device; (c) whether Defendant derives a benefit or information from the illegal use of an eavesdropping device; (d) whether Defendant directed another to use an eavesdropping device illegally on its behalf; (e) whether Session Replay Code is an “eavesdropping device” used to intercept or record private electronic communications; (f) whether Defendant acquired the contents of website users’ private electronic communications without their consent; (g) whether Plaintiff and Class members had a reasonable expectation of privacy in their Website communications; (f) whether Defendant violated the Illinois Eavesdropping Act 720 ILCS 5/14-1, *et seq.*; (g) whether Defendant’s interception of Plaintiff’s and Class members’ private electronic communications is an unfair or deceptive act or practice; (h) whether Zillow’s conduct violates the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.* (i) whether Plaintiff and the Class members are entitled to equitable relief; and (j) whether Plaintiff and the Class members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

61. **Typicality:** Plaintiff’s claims are typical of the other Class members’ claims because, among other things, all Class members were comparably injured through the uniform prohibited conduct described above. For instance, Plaintiff and each member of the Class had their electronic communications intercepted in violation of the law and their right to privacy. This uniform injury and the legal theories that underpin recovery make the claims of Plaintiff and the members of the Class typical of one another.

62. **Adequacy of Representation:** Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiff has no interest that is antagonistic to the interests of the Class, and Defendant

has no defenses unique to any Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiff nor his counsel have any interest adverse to the interests of the other members of the Class.

63. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

64. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant intercepted Plaintiff's and Class members' Website Communications, then Plaintiff and each Class member suffered damages by that conduct.

65. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class members may be readily identified through Zillow's books and records or the Session Replay Providers' books and records.

COUNT I
Violation of Illinois Eavesdropping Act
720 ILCS 5/14-1, *et seq.*

66. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

67. Plaintiff brings this claim individually and on behalf of the Class.

68. The Illinois Eavesdropping Act (the “Act”) prohibits (1) using an eavesdropping device in a surreptitious manner to overhear, transmit, or record all or any part of any private conversation; (2) intercepting, recording, or transcribing, in a surreptitious manner, any private electronic communication without consent; (3) manufacturing, assembling, distributing, or possessing any electronic, mechanical, eavesdropping, or other device knowing that or having reason to know that the design of the device renders it primarily useful for the purpose of surreptitious overhearing, transmitting, or recording of private conversations or the intersection; or (4) using or disclosing any information which he or she knows or reasonably should know was obtained from a private conversation or private electronic communication without the consent of all parties to the private electronic communication. 720 ILCS 5/14-2.

69. Any party to any conversation or private electronic communication upon which eavesdropping was practiced shall be entitled to (1) an injunction to prohibit further eavesdropping; (2) actual damages; and (3) punitive damages. punitive damages; 720 ILCS 5/14-6.

70. “Eavesdropping device” is defined as any “any device capable of being used to hear or record oral conversation or intercept, or transcribe electronic communications whether such conversation or electronic communication is conducted in person, by telephone, or by any other means[.]” 720 ILCS 5/14-1(a).

71. “Eavesdropper” is defined as “any person, including any law enforcement officer and any party to a private conversation, who operates or participates in the operation of any eavesdropping device contrary to the provisions of this Article or who acts as a principal, as defined in this Article.” 720 ILCS 5/14-1(b).

72. “Principle” is defined as “any person who: (1) knowingly employs another who illegally uses an eavesdropping device in the course of such employment; or (2) knowingly derives any benefit or information from the illegal use of an eavesdropping device by another; or (3) directs another to use an eavesdropping device illegally on his or her behalf.” 720 ILCS 5/14-1(c).

73. “Private electronic communication” is defined as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation. A reasonable expectation shall include any expectation recognized by law, including, but not limited to, an expectation derived from a privilege, immunity, or right established by common law, Supreme Court rule, or the Illinois or United States Constitution.” ILCS 5/14-1(e).

74. “Surreptitious” is defined as being “obtained or made by stealth or deception, or executed through secrecy or concealment.” 720 ILCS 5/14-1(g).

75. Zillow is an “Eavesdropper” and “Principal” for purposes of the Act because it operates or participates in the operation of an eavesdropping device, knowingly employs another who illegally uses an eavesdropping device, derives a benefit or information from the illegal use of an eavesdropping device, and directs another to use an eavesdropping device illegally on its behalf.

76. Session Replay Code like that operated and employed at Zillow’s direction is a “eavesdropping device” used to transcribe electronic communications within the meaning of the Act.

77. The Session Replay Providers are not a party to the Website Communications—Plaintiff and the Class only knew they were communicating with Zillow, not the Session Replay Providers.

78. Plaintiff's and Class members' intercepted Website Communications constitute the private electronic communications and private conversations within the meaning of the Act.

79. Zillow intentionally operated and employed Session Replay Code on its website to spy on, automatically and secretly, and intercept its website visitors' private electronic interactions communications with Zillow in real time.

80. Plaintiff's and Class members' private electronic communications were intercepted contemporaneously with their transmission.

81. Plaintiff and Class members had a reasonable expectation of privacy in their Website Communications based on the detailed information the Session Replay Code collected from Plaintiff and Class members.

82. Plaintiff and Class members did not consent to having their Website Communications surreptitiously intercepted and recorded.

83. Pursuant to 720 ILCS 5/14-6, Plaintiff and members of the Class are entitled to: (1) an injunction to prohibit further eavesdropping; (2) actual damages; and (3) punitive damages.

84. Zillow's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT II

**Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act
815 ILCS 505/1 *et seq.***

85. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

86. Plaintiff brings this claim individually and on behalf of the Class.

87. The Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.* (“ICFA”) protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

88. The ICFA prohibits “unfair or deceptive acts or practices,” including “misrepresentation or the concealment, suppression or omission of any material fact.” 815 ILCS 505/2.

89. The ICFA applies to Zillow’s conduct described herein because it protects consumers in transactions that are intended to result, or which have resulted in the sale of goods or services.

90. Zillow is a “person” within the meaning of ILCS 505/1(c) because it is a corporation.

91. Plaintiff and members of the Class are “consumers” within the meaning of 815 ILCS 505/1(e) because they visited www.zillow.com to shop for, purchase, or contract to purchase “merchandise”—real estate—for their own use.

92. Zillow’s advertising, offering for sale, and sale of real estate on www.zillow.com is considered “trade” or “commerce” within the meaning of 815 ILCS 505/1(f).

93. Zillow violated the ICFA by concealing material facts about www.zillow.com. Specifically, Zillow omitted and concealed that it directed Session Replay Providers to secretly

monitor, collect, transmit, and discloses its website visitors' Website Communications to the Session Replay Providers using Session Replay Code.

94. Zillow's direction and employment of the Session Replay Providers and their Session Replay Codes to intercept, collect, and disclose website visitors' Website Communications are material to the transactions on www.zillow.com. Zillow is leading online residential real estate marketplace in the United States and Zillow does not disclose its use of Session Replay Code to secretly monitor and collect website visitors' Website Communications. Had Plaintiff and the Class members known that the Session Replay Codes (that collect, transmit, and disclose Website Communications to the Session Replay Providers) were embedded in Zillow's website, they would not have visited www.zillow.com to shop for, purchase, or contract to purchase real estate or they would have required Zillow to compensate them for the interception, collection, and disclosure of their Website Communications.

95. Zillow's intentionally concealed the interception, collection, and disclosure of website visitors' Website Communications using Session Replay Code embedded in www.zillow.com is material because it knows that consumers would not otherwise visit its website to search for, purchase, and contract to purchase real estate. Indeed, Zillow's concealment of such facts was intended to mislead consumers.

96. Zillow's concealment, suppression, and omission of material facts was likely to mislead reasonable consumers under the circumstances, and thus constitutes an unfair and deceptive trade practice in violation of the ICFA.

97. By failing to disclose and inform Plaintiff and the Class about its interception, collection, and disclosure of website visitors' Website Communications, Zillow violated section 505/2 of the ICFA.

98. As a direct and proximate result of these unfair and deceptive practices, Plaintiff and each Class member has suffered actual harm in the form of money and/or property because the disclosure of their Website Communications has value as demonstrated by the collection and use of it by Zillow. The collection and use of this information has now diminished the value of such information to Plaintiff and the Class.

99. As such, Plaintiff and the Class seek an order (1) requiring Zillow to cease the unfair practices described herein; (2) awarding actual damages; and (3) awarding reasonable attorneys' fees and costs.

100. Zillow's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT III
Invasion of Privacy – Intrusion Upon Seclusion

101. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

102. Illinois common law recognizes the tort of invasion of privacy. The right to privacy is also embodied in the Illinois constitution.

103. Plaintiff brings this claim individually and on behalf of the Class.

104. Plaintiff and Class members had an objective, reasonable expectation of privacy in their Website Communications.

105. Plaintiff and Class members did not consent to, authorize, or know about Zillow's intrusion at the time it occurred. Plaintiff and Class members never agreed that Zillow could collect or disclose their Website Communications.

106. Plaintiff and Class members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

107. Zillow intentionally intruded on Plaintiff's and Class members' private life, seclusion, or solitude, without consent.

108. Zillow's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

109. Plaintiff and Class members were harmed by Zillow's wrongful conduct as Zillow's conduct has caused Plaintiff and the Class mental anguish and suffering arising from their loss of privacy and confidentiality of their electronic communications.

110. Zillow's conduct has needlessly harmed Plaintiff and the Class by capturing intimately personal facts and data in the form of their Website Communications. This disclosure and loss of privacy and confidentiality has caused Plaintiff and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

111. Additionally, given the monetary value of individual personal information, Defendant deprived Plaintiff and Class members of the economic value of their interactions with Defendant's website, without providing proper consideration for Plaintiff's and Class members' property.

112. Further, Zillow has improperly profited from its invasion of Plaintiff and Class members' privacy in its use of their data for its economic value.

113. As a direct and proximate result Zillow's conduct, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

114. Zillow's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with session replay software enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

REQUEST FOR RELIEF

Plaintiff, individually and on behalf of the other members of the proposed Class, respectfully requests that the Court enter judgment in Plaintiff's and the Class's favor and against Defendant as follows:

- A. Certifying the Class and appointing Plaintiff as the Class representative;
- B. Appointing Plaintiff's counsel as class counsel;
- C. Declaring that Defendant's past conduct was unlawful, as alleged herein;
- D. Declaring Defendant's ongoing conduct is unlawful, as alleged herein;
- E. Enjoining Defendant from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;
- F. Awarding Plaintiff and the Class members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;
- G. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

H. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

I. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the Class, demands a trial by jury of any and all issues in this action so triable of right.

Dated: September 8, 2022

Respectfully submitted,

/s/ Jonathan M. Jagher

Jonathan M. Jagher

**FREED KANNER LONDON
& MILLEN LLC**

923 Fayette Street

Conshohocken, Pennsylvania 19428

(610) 234-6486

jjagher@fklmlaw.com

Douglas A. Millen

Michael E. Moskovitz

**FREED KANNER LONDON
& MILLEN LLC**

2201 Waukegan Road, Ste. 130

Bannockburn, IL 60015

(224) 632-4500

dmillen@fklmlaw.com

mmoskovitz@fklmlaw.com

[Query](#) [Reports](#) [Utilities](#) [Help](#) [Log Out](#)

FUENTES

United States District Court
Northern District of Illinois - CM/ECF NextGen 1.6.3 (Chicago)
CIVIL DOCKET FOR CASE #: 1:22-cv-04847

Margulis v. Zillow Group, Inc.
Assigned to: Honorable Edmond E. Chang
Demand: \$9,999,000
Cause: Civil Miscellaneous Case

Date Filed: 09/08/2022
Jury Demand: Plaintiff
Nature of Suit: 360 P.I.: Other
Jurisdiction: Diversity

Plaintiff

Ryan Margulis
individually and on behalf of all others
similarly situated

represented by **Jonathan Marc Jagher**
Freed Kanner London & Millen Llc
923 Fayette Street
Conshohocken, PA 19428
United Sta
(610) 234-6486
Fax: Not a member
Email: jjagher@fklmlaw.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

V.

Defendant

Zillow Group, Inc.

Date Filed	#	Docket Text
09/08/2022	1	COMPLAINT filed by Ryan Margulis; Jury Demand. Filing fee \$ 402, receipt number AILNDC-19820397.(Jagher, Jonathan) (Entered: 09/08/2022)
09/08/2022	2	CIVIL Cover Sheet (Jagher, Jonathan) (Entered: 09/08/2022)
09/08/2022		CASE ASSIGNED to the Honorable Edmond E. Chang. Designated as Magistrate Judge the Honorable Gabriel A. Fuentes. Case assignment: Random assignment. (smb,) (Entered: 09/08/2022)
09/08/2022		CLERK'S NOTICE: Pursuant to Local Rule 73.1(b), a United States Magistrate Judge of this court is available to conduct all proceedings in this civil action. If all parties consent to have the currently assigned United States Magistrate Judge conduct all proceedings in this case, including trial, the entry of final judgment, and all post-trial proceedings, all parties must sign their names on the attached Consent To form. This consent form is eligible for filing only if executed by all parties. The parties can also express their consent to jurisdiction by a magistrate judge in any joint filing, including the Joint Initial Status Report or proposed Case Management Order. (smb,) (Entered: 09/08/2022)
09/08/2022	3	ATTORNEY Appearance for Plaintiff Ryan Margulis by Jonathan Marc Jagher (Jagher, Jonathan) (Entered: 09/08/2022)

09/26/2022	4	MINUTE entry before the Honorable Edmond E. Chang: Initial tracking status hearing set for 11/04/2022 at 8:30 a.m. to track the case only (no appearance is required, the case will not be called). Instead, the Court will set the case schedule after reviewing the written status report. The parties must file a joint initial status report with the content described in the attached status report requirements by 10/27/2022. Plaintiff must still file the report even if Defendant has not responded to requests to craft a joint report. If Defendant has not been served, then Plaintiff must complete the part of the report on the progress of service. Also, counsel (or the parties, if proceeding pro se) must carefully review Judge Chang's Case Management Procedures, available online at ilnd.uscourts.gov (navigate to Judges / District Judges / Judge Edmond E. Chang). Because the Procedures are occasionally revised, counsel (or the party, if proceeding pro se) must read them anew even if the counsel or the party has appeared before Judge Chang in other cases. Emailed notice (Attachments: # 1 Status Report Requirements) (mw,) (Entered: 09/26/2022)
09/28/2022		SUMMONS Issued as to Defendant Zillow Group, Inc. (ey,) (Entered: 09/28/2022)
09/29/2022	5	WAIVER OF SERVICE returned executed by Ryan Margulis. Zillow Group, Inc. waiver sent on 9/28/2022, answer due 11/28/2022. (Jagher, Jonathan) (Entered: 09/29/2022)
10/05/2022	6	MINUTE entry before the Honorable Edmond E. Chang: Given the answer deadline of 11/28/2022, R. 5, the tracking status hearing of 11/04/2022 is reset to 12/16/2022 at 8:30 a.m., but to track the case only (no appearance is required, the case will not be called). Instead, the parties shall file the joint initial status report by 12/08/2022. Emailed notice (mw,) (Entered: 10/05/2022)

PACER Service Center			
Transaction Receipt			
10/19/2022 10:38:17			
PACER Login:	samanthasouthall	Client Code:	0106198-000001-SS
Description:	Docket Report	Search Criteria:	1:22-cv-04847
Billable Pages:	2	Cost:	0.20

Multiple Documents

Part	Description
1	Main Document
2	Civil Cover Sheet

Joshua B. Swigart (SBN 225557)
 Josh@SwigartLawGroup.com
SWIGART LAW GROUP, APC
 2221 Camino del Rio S, Ste 308
 San Diego, CA 92108
 P: 866-219-3343

*Attorneys for Plaintiff
 and The Putative Class*

Daniel G. Shay (SBN 250548)
 DanielShay@TCPAFDCPA.com
LAW OFFICE OF DANIEL G. SHAY
 2221 Camino del Rio S, Ste 308
 San Diego, CA 92108
 P: 619-222-7429

**UNITED STATES DISTRICT COURT
 SOUTHERN DISTRICT OF CALIFORNIA**

DAVID KAUFFMAN, individually and
 on behalf of others similarly situated,

Plaintiff,

vs.

ZILLOW GROUP, INC.,

Defendant.

CASE NO: '22CV1398 LL AGS

CLASS ACTION

COMPLAINT FOR DAMAGES:

UNLAWFUL WIRETAPPING AND
 INTERCEPTION OF ELECTRONIC
 COMMUNICATIONS, CAL. PEN.
 CODE § 631

JURY TRIAL DEMANDED

INTRODUCTION

1. David Kauffman (“Plaintiff”), individually and on behalf of all other similarly situated California residents (“Class Members”), brings this action for damages and injunctive relief against Zillow Group, Inc. (“Defendant”), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, related entities for violations of the California Penal Code § 631 Wiretapping, (“CIPA”) in relation to the unauthorized collection, recording, and dissemination of Plaintiff’s and Class Members’ data.
2. The California State Legislature passed CIPA to protect the right of privacy of the people of California. The California Penal Code is very clear in its prohibition against unauthorized tapping or connection without the consent of the other person:

“Any person who, by means of any machine, instrument, or contrivance, or any other matter, intentionally taps, or makes any unauthorized connection . . . with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable. Or instrument of any internal telephonic communication system, or who willfully and without consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state [violates this section].”
Cal. Penal Code § 631(a).
3. This case stems from Defendant’s unauthorized connection to Plaintiff’s and Class Members’ electronic communications through the use of “session replay” spyware that allowed Defendant to read, learn the contents of, and report Plaintiff’s and Class Members’ visits to Defendant’s websites.
4. Plaintiff brings this action for every violation of California Penal Code § 631 which provides for statutory damages of \$2,500 for each violation, pursuant to California Penal Code § 631(a).

///

- 1 5. As discussed in detail below, Defendant utilized “session replay” spyware to
2 intercept Plaintiff’s and the Class Members’ electronic computer-to-computer
3 data communications, including how Plaintiff and Class Members interacted with
4 the website, mouse movements and clicks, keystrokes, search items, information
5 inputted into the website, and pages and content viewed while visiting the
6 website. Defendant intentionally tapped and made unauthorized connection to
7 Plaintiff and Class Members’ electronic communications to read and understand
8 movement on the website, as well as everything Plaintiff and Class Members did
9 on those pages, *e.g.*, what Plaintiff and Class Members searched for, looked at,
10 the information inputted, and clicked on.
- 11 6. Defendant made this unauthorized connection without the knowledge or prior
12 consent of Plaintiff of Class Members.
- 13 7. The “session replay” spyware utilized by Defendant is a sophisticated computer
14 software that allows Defendant to contemporaneously intercept, capture, read,
15 observe, re-route, forward, redirect, and receive electronic communications.
- 16 8. “Technological advances[,]” such as Defendant’s use of “session replay”
17 technology, “provide ‘access to a category of information otherwise unknowable’
18 and ‘implicate privacy concerns’ in a manner different from traditional intrusions
19 as a ‘ride on horseback’ is different from a ‘flight to the moon.’” *Patel v.*
20 *Facebook, Inc.*, 932 F.3d 1264, 1273 (9th Cir. 2019) (quoting *Riley v. California*,
21 573 U.S. 373, 393 (2014)).
- 22 9. Jonathan Cherki, the CEO of a major “session replay” spyware company – while
23 discussing the merger of his company with another “session replay” provider –
24 publicly exposed why companies like Defendant engage in learning the contents
25 of visits to their websites: “The combination of Clicktale and Contentsquare
26 heralds an unprecedented goldmine of digital data that enables companies to
27 interpret and predict the impact of any digital element – including user
28

1 experience, content, price, reviews and product – on visitor behavior[.]”¹ Mr.
2 Cherki added that, “this unique data can be used to activate custom digital
3 experiences in the moment via an ecosystem of over 50 martech partners. With a
4 global community of customer and partners, we are accelerating the
5 interpretation of human behavior online and shaping a future of addictive
6 customer experience.”²

7 10. Unlike typical website analytics services that provide aggregate statistics, the
8 session replay technology utilized by Defendant is intended to record and
9 playback individual browsing session, as if someone is looking over Plaintiff’s
10 or a Class Members’ shoulder when visiting Defendant’s website. The
11 technology also permits companies like Defendant to view the interactions of
12 visitors on Defendant’s website in live, real-time.

13 11. The purported use of “session replay” technology is to monitor and discover
14 broken website features; however, the extent and detail collected by users of the
15 technology, like Defendant, far exceeds the stated purpose and Plaintiff’s and
16 Class Members’ expectations when visiting websites like Defendant’s. The
17 technology not only allows the tapping and unauthorized connection of a visitor’s
18 electronic communication with a website, but also allows the user to create a
19 detailed profile for each visitor to the site.

20 12. Moreover, the collection and storage of page content may cause sensitive
21 information and other personal information displayed on a page to lead to third
22 parties. This may expose website visitors to identity theft, online scams, and other
23 unwanted behavior.

24 13. In 2019, Apple warned application developers using “session replay” technology
25 that they were required to disclose such action to their users, or face being

26
27 ¹ [https://www.prnewswire.com/news-releases/contentsquare-acquires-clicktale-to-create-the-](https://www.prnewswire.com/news-releases/contentsquare-acquires-clicktale-to-create-the-definitive-global-leader-in-experience-analytics-300878232.html)
28 [definitive-global-leader-in-experience-analytics-300878232.html](https://www.prnewswire.com/news-releases/contentsquare-acquires-clicktale-to-create-the-definitive-global-leader-in-experience-analytics-300878232.html)

² *Id*

immediately removed from the Apple Store: “Protecting user privacy is paramount in the Apple ecosystem. Our App Store Review Guidelines require that apps request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity.”³

14. Consistent with Apple’s concerns, countless articles have been written about the privacy implications of recording user interactions during a visit to a website, including:

(a) *The Dark Side of ‘Replay Sessions’ That Record Your Every Move Online*,

located at <https://www.wired.com/story/the-dark-side-of-replay-sessions-that-record-your-every-move-online/>;

(b) *Session-Replay Scripts Disrupt Online Privacy in a Big Way*, located at

<https://www.techrepublic.com/article/session-replay-scripts-are-disrupting-online-privacy-in-a-big-way/>;

(c) *Are Session Recording Tools a Risk to Internet Privacy?* located at

<https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/>

(d) *Session Replay is a Major Threat to Privacy on the Web*, located at

<https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720>;

(e) *Popular Websites Record Every Keystroke You Make and Put Personal*

Information and Risk, located at <https://medium.com/stronger-content/popular-websites-record-every-keystroke-you-make-and-put-personal-information-at-risk-c5e95dfda514>; and

(f) *Website Owners can Monitor Your Every Scroll and Click*, located at

<https://www.digitalinformationworld.com/2020/02/top-brands-and-websites-can-monitor-your-every-scroll-and-click.html>

³ <https://techcrunch.com/2019/02/07/apple-glassbox-apps/>

1 15. In sum, Defendant illegally tapped and made an unauthorized connection to
2 Plaintiff's and Class Members' electronic communications through visits to
3 Defendant's website, causing injuries, including violations of Plaintiff's and
4 Class Members' substantive legal privacy rights under CIPA, invasion of
5 privacy, and potential exposure of private information.

6 16. Plaintiff makes these allegations on information and belief, with the exception of
7 those allegations that pertain to Plaintiff, or to Plaintiff's counsel, which Plaintiff
8 alleges on his personal knowledge.

9 17. Unless otherwise stated, all the conduct engaged in by Defendant took place in
10 California.

11 18. All violations by Defendant were knowing, willful, and intentional, and
12 Defendant did not maintain procedures reasonably adapted to avoid any such
13 violation.

14 19. Unless otherwise indicated, the use of Defendant's name in this Complaint
15 includes all agents, employees, officers, members, directors, heirs, successors,
16 assigns, principals, trustees, sureties, subrogees, representatives, and insurers of
17 the named Defendant.

18 **PARTIES**

19 20. Plaintiff is, and at all times mentioned herein was, a natural person and resident
20 of the State of California and the County of San Diego.

21 21. Defendant is, and at all times mentioned herein was, a Washington corporation
22 with its principal place of business located at 1301 Second Avenue Floor 31,
23 Seattle, WA 98101.

24 22. At all times relevant herein Defendant conducted business in the State of
25 California, in the County of San Diego, within this judicial district.

26 ///

27 ///

28 ///

JURISDICTION & VENUE

23. Jurisdiction is proper under the Class Action Fairness Act (“CAFA”), 28 U.S.C. § 1332(d)(2), because Plaintiff, a resident of the State of California, seeks relief on behalf of a California class, which will result in at least one Class Member belonging to a different state than Defendant, a Washington Corporation with its principal place of business in Washington.
24. Plaintiff is requesting statutory damages of \$2,500 per violation of Cal. Penal Code §631, which, when aggregated among a proposed class number in the tens of thousands, exceeds the \$5,000,000 threshold for federal court jurisdiction under CAFA.
25. Therefore, both diversity jurisdiction and the damages threshold under CAFA are present, and this Court has jurisdiction.
26. Because Defendant conducts business within the State of California, personal jurisdiction is established.
27. Venue is proper pursuant to 28 U.S.C. § 1391 for the following reasons: (i) the conduct complained of herein occurred within this judicial district; and (ii) Defendant conducted business within this judicial district at all times relevant.

FACTUAL ALLEGATIONS

28. Defendant owns and operates the following website: www.zillow.com.
29. Over the past year, Plaintiff and Class members visited Defendant’s website.
30. Plaintiff was in California during each visit to Defendant’s website.
31. During visits to the website, Plaintiff and Class Members, through computers and/or mobile devices, transmitted electronic communications in the form of instructions to Defendant’s computer servers utilized to operate the website. The commands were sent as messages indicating to Defendant what content was being viewed, clicked on, requested and/or inputted by Plaintiff and Class Members. The communications sent by Plaintiff and Class Members to Defendant’s servers included, but were not limited to, the following actions taken

1 by Plaintiff and Class Members while on Defendant’s website: mouse clicks and
2 movements, keystrokes, search items, information inputted by Plaintiff and Class
3 Members, pages and content viewed by Plaintiff and Class Members, scroll
4 movements, and copy and paste actions.

5 32. Defendant responded to Plaintiff’s and Class Members’ electronic
6 communications by supplying – through its website – the information requested
7 by Plaintiff and Class Members. *Revitch v. New Moosejaw, LLC*, U.S. Dist.
8 LEXIS 186955, at *3 (N.D. Cal. 2019) (“This series of requests and responses –
9 whether online or over the phone – is communication.”).

10 33. Plaintiff and Class Members reasonably expected that visits to Defendant’s
11 website would be private, and that Defendant would not be tapping, connecting
12 with, or otherwise attempting to understand their communications with
13 Defendant’s website, particularly because Defendant failed to present Plaintiff
14 and Class Members with a pop-up disclosure or consent form alerting Plaintiff
15 that the visits to the website were monitored and recorded by Defendant.

16 34. Plaintiff and Class Members reasonably believed their interactions with
17 Defendant’s website were private and would not be recorded or monitored for a
18 later playback by Defendant, or worse yet, live monitoring while Plaintiff and
19 Class Members were on the website.

20 35. Upon information and belief, over the last few years, Defendant has had
21 embedded within its website code and has continuously operated at least one
22 “session replay” script that was provided by a third party (“Session Replay
23 Provider”). The “session replay” spyware was always active and intercepted
24 every incoming data communication to Defendant’s website the moment a visitor
25 accessed the site.

26 36. The Session Replay Provider(s) that provided that “session replay” spyware to
27 Defendant is not a provider of wire or electronic communication services, or an
28 internet service provider.

37. Defendant's use of "session play" spyware was not instrumental or necessary to the operation or function of Defendant's website or business.

38. Defendant's use of "session replay" spyware to intercept Plaintiff's electronic communications was not instrumental or necessary to Defendant's provision of any of its goods or services. Rather, the level and detail of information surreptitiously collected by Defendant indicates that the only purpose was to gain an unlawful understanding of the habits and preferences of users to its websites, and the information collected was solely for Defendant's own benefit.

39. Defendant's use of a "session replay" spyware to intercept Plaintiff's and Class Members' electronic communications did not facilitate, was not instrumental, and was not incidental to the transmission of Plaintiff's and Class Members' electronic communications with Defendant's website.

40. During one or more of Plaintiff's and Class Members' visits to Defendant's website, Defendant utilized "session replay" spyware to intercept the substance of Plaintiff's and Class Members' electronic communications intentionally and contemporaneously with Defendant's website, including mouse clicks and movements, keystrokes, search terms, information inputted by Plaintiff, pages and content viewed, scroll movements, and copy and paste actions. In other words, Defendant tapped and made an unauthorized connection with the electronic communications Plaintiff and Class Members made during visits to Defendant's website.

41. The relevant facts regarding the full parameters of the communications Defendant made an unauthorized connection with and the extent to of how the connections occurred are solely within the possession and control of the Defendant.

42. The "session replay" spyware utilized by Defendant is not a website cookie, standard analytics tool, web beacon, or other similar technology.

///

43. Unlike harmless collection of an internet protocol address, the data collected by Defendant identified specific information inputted and content viewed, and thus revealed personalized and sensitive information about Plaintiff's and Class Member's internet activity and habits.

44. The electronic communications Defendant intentionally made an unauthorized connection was content generated through Plaintiff's intended use, interaction, and communication with Defendant's website relating to the substance, purport, and/or meaning of Plaintiff's and Class Members' communications with the website.

45. The electronic communications Defendant made and unauthorized connection with were not generated automatically and were not incidental to Plaintiff's and Class Members' communications.

46. The "session replay" spyware utilized by Defendant tapped, made an unauthorized connection, which allowed Defendant to attempt to learn the communications of Plaintiff and Class Members in a manner that was undetectable by Plaintiff.

47. Plaintiff's electronic data communications were then stored by Defendant, which Defendant could use to playback Plaintiff's and Class Members' interactions with Defendant's website.

48. Defendant never sought consent and Plaintiff and Class Members never provided consent for Defendant's unauthorized access to Plaintiff's and Class Members' electronic communications.

49. Plaintiff and Class Members did not have a reasonable opportunity to discover Defendant's unlawful and unauthorized connections because Defendant did not disclose its actions nor seek consent from Plaintiff and Class Members prior to making the unauthorized connection to the electronic communications through the "session replay" spyware.

///

50. Plaintiff and Class Members were not placed on notice of Defendant's terms and policies or privacy policy immediately visiting the website. Instead, Defendant's terms of use and privacy policy are buried at the bottom of Defendant's website, out of site from Plaintiff and Class Members.

51. Defendant does not require visitors to its websites to immediately and directly acknowledge that the visitor has read Defendant's terms of use or privacy policy before proceeding to the site.

52. Defendant's purpose and use of the "session replay" spyware is to attempt to understand Plaintiff's and Class Members' electronic communications with Defendant's website.

STANDING

53. Defendant's conduct constituted invasions of privacy because it disregarded Plaintiff's statutorily protected rights to privacy, in violation of CIPA.

54. Defendant caused Plaintiff to (1) suffer invasions of legally protected interests. (2) The invasions were concrete because the injuries actually existed for Plaintiff and continue to exist every time Plaintiff visits Defendant's website. The privacy invasions suffered by Plaintiff and the Class were real and not abstract. Plaintiff and the Class have a statutory right to be free from interceptions of their communications. The interceptions Defendant performed were meant to secretly spy on Plaintiff to learn more about Plaintiff's behavior. Plaintiff and Class members were completely unaware they were being observed. Plaintiffs' injuries were not divorced from concrete harm in that privacy has long been protected in the form of trespassing laws and the Fourth Amendment of the U.S. Constitution for example. Like here, an unreasonable search may not cause actual physical injury, but is considered serious harm, nonetheless. (3) The injuries here were particularized because they affected Plaintiff in personal and individual ways. The injuries were individualized rather than collective since Plaintiff's unique communications were examined without consent during different website visits

on separate occasions. (4) Defendant's past invasions were actual and future invasions are imminent and will occur next time Plaintiff visits Defendant's website. Defendant continues to intercept communications in California without consent. A favorable decision by this court would redress the injuries of Plaintiff and the Class.

TOLLING

55. Any applicable statute(s) of limitations has been tolled by the "delayed discovery" rule. Plaintiff did not know (and had no way of knowing) that his information was intercepted, because Defendant kept this information secret.

CLASS ACTION ALLEGATIONS

56. Plaintiff brings this lawsuit as a class action on behalf of himself and Class Members of the proposed Class. This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of those provisions.

57. Plaintiff proposes the following Class, consisting of and defined as follows:

All persons in California whose communications were intercepted by Defendant, and or its agents.

58. Excluded from the Class are: (1) Defendant, any entity or division in which Defendant has a controlling interest, and its legal representatives, officers, directors, assigns, and successors; (2) the Judge to whom this case is assigned and the Judge's staff; and (3) those persons who have suffered personal injuries as a result of the facts alleged herein. Plaintiff reserves the right to redefine the Class and to add subclasses as appropriate based on discovery and specific theories of liability.

59. **Numerosity**: The Class Members are so numerous that joinder of all members would be unfeasible and impractical. The membership of the entire Class is currently unknown to Plaintiff at this time; however, given that, on information and belief, Defendant accessed millions of unique computers and mobile devices,

1 it is reasonable to presume that the members of the Class are so numerous that
2 joinder of all members is impracticable. The disposition of their claims in a class
3 action will provide substantial benefits to the parties and the Court.

4 ///

5 60. **Commonality**: There are common questions of law and fact as to Class Members
6 that predominate over questions affecting only individual members, including,
7 but not limited to:

- 8 • Whether, within the statutory period, Defendant intercepted any
9 communications with Class Members;
- 10 • Whether Defendant had, and continues to have, a policy during the
11 relevant period of intercepting digital communications of Class
12 Members;
- 13 • Whether Defendant's policy or practice of intercepting Class
14 Members digital communications constitutes a violation of Cal.
15 Penal Code § 631;
- 16 • Whether Plaintiff and Class Members were aware of Defendant's
17 "session replay" spyware and had consented to its use.

18 61. **Typicality**: Plaintiff's and Class Members' wire and cellular telephone
19 communications were intercepted, unlawfully tapped and recorded without
20 consent or a warning of such interception and recording, and thus, his injuries are
21 also typical to Class Members.

22 62. Plaintiff and Class Members were harmed by the acts of Defendant in at least the
23 following ways: Defendant, either directly or through its agents, illegally
24 intercepted, tapped, recorded, and stored Plaintiff and Class Members' electronic
25 communications, and other sensitive personal data from their digital devices with
26 others, and Defendant invading the privacy of said Plaintiff and Class. Plaintiff
27 and Class Members were damaged thereby.
28

63. **Adequacy**: Plaintiff is qualified to, and will, fairly and adequately protect the interests of each Class Member with whom he is similarly situated, as demonstrated herein. Plaintiff acknowledges that he has an obligation to make known to the Court any relationships, conflicts, or differences with any Class Member. Plaintiff's attorneys, the proposed class counsel, are versed in the rules governing class action discovery, certification, and settlement. In addition, Plaintiff's attorneys, the proposed class counsel, are versed in the rules governing class action discovery, certification, and settlement. The proposed class counsel is experienced in handling claims involving consumer actions and violations of the California Penal Code § 631. Plaintiff has incurred, and throughout the duration of this action, will continue to incur costs and attorneys' fees that have been, are, and will be, necessarily expended for the prosecution of this action for the substantial benefit of each Class Member.

64. **Predominance**: Questions of law or fact common to the Class Members predominate over any questions affecting only individual members of the Class. The elements of the legal claims brought by Plaintiff and Class Members are capable of proof at trial through evidence that is common to the Class rather than individual to its members.

65. **Superiority**: A class action is a superior method for the fair and efficient adjudication of this controversy because:

a. Class-wide damages are essential to induce Defendant to comply with California and Federal law.

b. Because of the relatively small size of the individual Class Members' claims, it is likely that only a few Class Members could afford to seek legal redress for Defendant's misconduct.

c. Management of these claims is likely to present significantly fewer difficulties than those presented in many class claims.

d. Absent a class action, most Class Members would likely find

1 the cost of litigating their claims prohibitively high and would
2 therefore have no effective remedy at law.

3 e. Class action treatment is manageable because it will permit a
4 large number of similarly situated persons to prosecute their
5 common claims in a single forum simultaneously, efficiently, and
6 without the unnecessary duplication of effort and expense that
7 numerous individual actions would endanger.

8 f. Absent a class action, Class Members will continue to incur
9 damages, and Defendant's misconduct will continue without
10 remedy.

11 66. Plaintiff and the Class Members have all suffered and will continue to suffer harm
12 and damages as a result of Defendant's unlawful and wrongful conduct. A class
13 action is also superior to other available methods because as individual Class
14 Members have no way of discovering that Defendant intercepted and recorded
15 the Class Member's telephonic electronic communications without Class
16 Members' knowledge or consent.

17 67. The Class may also be certified because:

- 18 • The prosecution of separate actions by individual Class Members
19 would create a risk of inconsistent or varying adjudication with
20 respect to individual Class Members, which would establish
21 incompatible standards of conduct for Defendant;
- 22 • The prosecution of separate actions by individual Class Members
23 would create a risk of adjudications with respect to them that
24 would, as a practical matter, be dispositive of the interests of other
25 Class Members not parties to the adjudications, or substantially
26 impair or impede their ability to protect their interests; and
- 27 • Defendant has acted or refused to act on grounds generally
28 applicable to the Class, thereby making appropriate final and

injunctive relief with respect to the members of the Class as a whole.

68. This suit seeks only damages and injunctive relief for recovery of economic injury on behalf of Class Members and it expressly is not intended to request any recovery for personal injury and claims related thereto.

69. The joinder of Class Members is impractical and the disposition of their claims in the Class action will provide substantial benefits both to the parties and to the court. The Class Members can be identified through Defendant's records.

CAUSE OF ACTION

UNLAWFUL WIRETAPPING AND INTERCEPTION OF ELECTRONIC COMMUNICATION

CALIFORNIA PENAL CODE § 631

70. Plaintiff repeats, re-alleges, and incorporates by reference, all other paragraphs.

71. At all relevant times to this complaint, Defendant intercepted components of Plaintiff's and the putative Class Members' private electronic communications and transmissions when Plaintiff and other Class Members accessed Defendant's website within the State of California.

72. At all relevant times to this complaint, Plaintiff and the other Class Members did not know Defendant was engaging in such interception and therefore could not provide consent to have any part of their private electronic communications intercepted by Defendant.

73. Plaintiff and Class Members were completely unaware that Defendant had intercepted and stored electronic communications and other personal data until well after the fact and was therefore unable to consent.

74. At the inception of Defendant's illegally intercepted and unauthorized connections to Plaintiff's and Class Members' electronic communications, Defendant never advised Plaintiff or the other Class Members that any part of this communications or their use of Defendant's website would be intercepted.

75. Plaintiff and Class Members were completely unaware that their use of Defendant's website and the electronic communications derived from the use was being intercepted and stored

///

///

///

76. To establish liability under section 631(a), a plaintiff need only establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner," does any of the following:

Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,

Or

Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,

Or

Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,

Or

Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

- 1
2 77. Section 631(a) is not limited to phone lines, but also applies to “new
3 technologies” such as computers, the Internet, and email. *Matera v. Google Inc.*,
4 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to “new
5 technologies” and must be construed broadly to effectuate its remedial purpose
6 of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5-6 (N.D.
7 Cal. Dec. 22, 2006) (CIPA governs “electronic communications”); *In re*
8 *Facebook, Inc. Internet Tracking Litigation*, --- F.3d --- 2020 WL 1807978 (9th
9 Cir. Apr. 9, 2020) (reversing dismissal of CIPA and common law privacy claims
10 based on Facebook’s collection of consumers’ Internet browsing history).
- 11 78. Defendant’s use of the “session replay” spyware is a “machine, instrument,
12 contrivance, or . . . other manner” used to engage in the prohibited conduct at
13 issue here.
- 14 79. At all relevant times, by using the “session replay” spyware to track, record, and
15 attempt to learn the contents of Plaintiff’s and Class Members’ electronic
16 communications, Defendant intentionally tapped, electrically or otherwise, the
17 lines of internet communication between Plaintiff and Class Members on the one
18 hand, and the specific sites and locations Plaintiffs and Class Members visited on
19 Defendant’s website on the other.
- 20 80. At all relevant times, by utilizing the “session replay” spyware, Defendant
21 willfully and without the consent of all parties to the communication, or in any
22 unauthorized manner, read or attempted to read or learn the contents or meaning
23 of electronic communications of Plaintiff and putative Class Members, while the
24 electronic communications were in transit or passing over any wire, line or cable
25 or were being sent from or received at any place within California.
- 26 81. Plaintiff and Class Members did not consent to any of Defendant’s actions in
27 implementing these unauthorized connections, nor have Plaintiff or Class
28 Members consented to Defendants’ intentional access, interception, reading,

learning, recording, and collection of Plaintiff's and Class Members' electronic communications.

///

///

///

///

82. Plaintiff's and the Class Members' devices that Defendant accessed through its unauthorized actions included their computers, smart phones, and tablets and/or other electronic computing devices.

83. Defendant violated Cal. Penal Code § 631 by knowingly accessing, and without permission accessing, Plaintiff's and Class Members' electronic communications through the use of the "session replay" spyware in order for Defendant to track, understand, and attempt to learn the contents of Plaintiff's and Class Members' electronic communications generated by the use of Defendant's website, in violation of Plaintiff's and Class Members' reasonable expectations of privacy in their devices and data.

84. Defendant violated Cal. Penal Code § 631 by knowingly and without permission intercepting, wiretapping, accessing, taking and using Plaintiff's and the Class Members' personally identifiable information and personal communications with others.

85. Plaintiff and Class Members seek all relief available under Cal. Penal Code § 631, including \$2,500 per violation.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class Members pray that judgment be entered against Defendant, and Plaintiff and Class Members be awarded damages from Defendant, as follows:

- Certify the Class as requested herein;
- Appoint Plaintiff to serve as the Class Representative for the Class; and

- Appoint Plaintiff's Counsel as Class Counsel in this matter for the Class.
- \$2,500 to each Class Member pursuant to California Penal Code § 631(a) for each unlawful interception of communications;
- Reasonable attorneys' fees pursuant to Cal. Code of Civ. Proc. § 1021.5;
- Injunctive relief to prevent the further occurrence of such illegal acts pursuant to California Penal Code § 631;
- An award of costs to Plaintiff; and
- Any other relief the Court may deem just and proper including interest.

TRIAL BY JURY

86. Pursuant to the Seventh Amendment to the Constitution of the United States of America, Plaintiff and Class Members are entitled to, and demand, a trial by jury.

Respectfully submitted,

SWIGART LAW GROUP

Date: September 15, 2022

By: s/ Joshua Swigart
Joshua B. Swigart, Esq.
Josh@SwigartLawGroup.com
Attorneys for Plaintiff

LAW OFFICE OF DANIEL G. SHAY

Date: September 15, 2022

By: s/ Daniel Shay
Daniel G. Shay, Esq.
DanielShay@TCPAFDCPA.com
Attorney for Plaintiffs

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

David Kauffman, individually and on behalf of others

(b) County of Residence of First Listed Plaintiff San Diego
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

Swigart Law Group, 2221 Camino Del Rio S, Ste 308
San Diego, CA 92108 - 866-219-3343 & Daniel Shay, Esq

DEFENDANTS

Zillow Group, Inc.

County of Residence of First Listed Defendant _____
(IN U.S. PLAINTIFF CASES ONLY)NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF
THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

'22CV1398 LL AGS

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff
- ☐ 2 U.S. Government Defendant
- ☐ 3 Federal Question
(U.S. Government Not a Party)
- ☒ 4 Diversity
(Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- | | PTF | DEF | | PTF | DEF |
|---|---------------------------------------|----------------------------|---|----------------------------|---------------------------------------|
| Citizen of This State | <input checked="" type="checkbox"/> 1 | <input type="checkbox"/> 1 | Incorporated or Principal Place of Business In This State | <input type="checkbox"/> 4 | <input type="checkbox"/> 4 |
| Citizen of Another State | <input type="checkbox"/> 2 | <input type="checkbox"/> 2 | Incorporated and Principal Place of Business In Another State | <input type="checkbox"/> 5 | <input checked="" type="checkbox"/> 5 |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3 | <input type="checkbox"/> 3 | Foreign Nation | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 |

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Click here for: [Nature of Suit Code Descriptions.](#)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
<input type="checkbox"/> 110 Insurance	PERSONAL INJURY	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881	<input type="checkbox"/> 422 Appeal 28 USC 158	<input type="checkbox"/> 375 False Claims Act
<input type="checkbox"/> 120 Marine	<input type="checkbox"/> 310 Airplane	<input type="checkbox"/> 690 Other	<input type="checkbox"/> 423 Withdrawal 28 USC 157	<input type="checkbox"/> 376 Qui Tam (31 USC 3729(a))
<input type="checkbox"/> 130 Miller Act	<input type="checkbox"/> 315 Airplane Product Liability		INTELLECTUAL PROPERTY RIGHTS	<input type="checkbox"/> 400 State Reapportionment
<input type="checkbox"/> 140 Negotiable Instrument	<input type="checkbox"/> 320 Assault, Libel & Slander		<input type="checkbox"/> 820 Copyrights	<input type="checkbox"/> 410 Antitrust
<input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment	<input type="checkbox"/> 330 Federal Employers' Liability		<input type="checkbox"/> 830 Patent	<input type="checkbox"/> 430 Banks and Banking
<input type="checkbox"/> 151 Medicare Act	<input type="checkbox"/> 340 Marine		<input type="checkbox"/> 835 Patent - Abbreviated New Drug Application	<input type="checkbox"/> 450 Commerce
<input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans)	<input type="checkbox"/> 345 Marine Product Liability		<input type="checkbox"/> 840 Trademark	<input type="checkbox"/> 460 Deportation
<input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits	<input type="checkbox"/> 350 Motor Vehicle	LABOR	<input type="checkbox"/> 880 Defend Trade Secrets Act of 2016	<input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations
<input type="checkbox"/> 160 Stockholders' Suits	<input type="checkbox"/> 355 Motor Vehicle Product Liability	<input type="checkbox"/> 710 Fair Labor Standards Act	SOCIAL SECURITY	<input type="checkbox"/> 480 Consumer Credit (15 USC 1681 or 1692)
<input type="checkbox"/> 190 Other Contract	<input type="checkbox"/> 360 Other Personal Injury	<input type="checkbox"/> 720 Labor/Management Relations	<input type="checkbox"/> 861 HIA (1395ff)	<input type="checkbox"/> 485 Telephone Consumer Protection Act
<input type="checkbox"/> 195 Contract Product Liability	<input type="checkbox"/> 362 Personal Injury - Medical Malpractice	<input type="checkbox"/> 740 Railway Labor Act	<input type="checkbox"/> 862 Black Lung (923)	<input type="checkbox"/> 490 Cable/Sat TV
<input type="checkbox"/> 196 Franchise		<input type="checkbox"/> 751 Family and Medical Leave Act	<input type="checkbox"/> 863 DIWC/DIWW (405(g))	<input type="checkbox"/> 850 Securities/Commodities/Exchange
REAL PROPERTY	CIVIL RIGHTS	<input type="checkbox"/> 790 Other Labor Litigation	<input type="checkbox"/> 864 SSID Title XVI	<input checked="" type="checkbox"/> 890 Other Statutory Actions
<input type="checkbox"/> 210 Land Condemnation	<input type="checkbox"/> 440 Other Civil Rights	<input type="checkbox"/> 791 Employee Retirement Income Security Act	<input type="checkbox"/> 865 RSI (405(g))	<input type="checkbox"/> 891 Agricultural Acts
<input type="checkbox"/> 220 Foreclosure	<input type="checkbox"/> 441 Voting		FEDERAL TAX SUITS	<input type="checkbox"/> 893 Environmental Matters
<input type="checkbox"/> 230 Rent Lease & Ejectment	<input type="checkbox"/> 442 Employment	IMMIGRATION	<input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant)	<input type="checkbox"/> 895 Freedom of Information Act
<input type="checkbox"/> 240 Torts to Land	<input type="checkbox"/> 443 Housing/Accommodations	<input type="checkbox"/> 462 Naturalization Application	<input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	<input type="checkbox"/> 896 Arbitration
<input type="checkbox"/> 245 Tort Product Liability	<input type="checkbox"/> 445 Amer. w/Disabilities - Employment	<input type="checkbox"/> 465 Other Immigration Actions		<input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision
<input type="checkbox"/> 290 All Other Real Property	<input type="checkbox"/> 446 Amer. w/Disabilities - Other			<input type="checkbox"/> 950 Constitutionality of State Statutes
	<input type="checkbox"/> 448 Education			
	PRISONER PETITIONS			
	Habeas Corpus:			
	<input type="checkbox"/> 463 Alien Detainee			
	<input type="checkbox"/> 510 Motions to Vacate Sentence			
	<input type="checkbox"/> 530 General			
	<input type="checkbox"/> 535 Death Penalty			
	Other:			
	<input type="checkbox"/> 540 Mandamus & Other			
	<input type="checkbox"/> 550 Civil Rights			
	<input type="checkbox"/> 555 Prison Condition			
	<input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN (Place an "X" in One Box Only)

- ☒ 1 Original Proceeding
- ☐ 2 Removed from State Court
- ☐ 3 Remanded from Appellate Court
- ☐ 4 Reinstated or Reopened
- ☐ 5 Transferred from Another District (specify)
- ☐ 6 Multidistrict Litigation - Transfer
- ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d) and California Invasion of Privacy Act (CIPA), Cal. Pen. Code 631 et seq.Brief description of cause:
Illegal interception of communications without consent.

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND \$

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE _____ DOCKET NUMBER _____

DATE

9/15/2022

SIGNATURE OF ATTORNEY OF RECORD

s/ Joshua B. Swigart

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I.(a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- (b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
- (c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
- United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here. United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
- Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
- Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).
- V. Origin.** Place an "X" in one of the seven boxes.
- Original Proceedings. (1) Cases which originate in the United States district courts.
- Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
- Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
- Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
- Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
- Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
- Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
- PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7.** Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.
- VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
- Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
- Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

[Query](#) [Reports](#) [Utilities](#) [Help](#) [Log Out](#)

**U.S. District Court
Southern District of California (San Diego)
CIVIL DOCKET FOR CASE #: 3:22-cv-01398-LL-AGS**

Kauffman v. Zillow Group, Inc.
Assigned to: Judge Linda Lopez
Referred to: Magistrate Judge Andrew G. Schopler
Cause: 28:1453 Class Action Fairness Act

Date Filed: 09/15/2022
Jury Demand: Plaintiff
Nature of Suit: 190 Contract: Other
Jurisdiction: Diversity

Plaintiff

David Kauffman
*individually and on behalf of others
similarly situated*

represented by **Daniel G. Shay**
Law Office of Daniel G. Shay
2221 Camino Del Rio South
Suite 308
San Diego, CA 92108
(619) 222-7429
Fax: (866) 431-3292
Email: DanielShay@TCPAFDCPA.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joshua Brandon Swigart
Swigart Law Group, APC
2221 Camino Del Rio South
Suite 308
San Diego, CA 92108
(866) 219-3343
Fax: (866) 219-8344
Email: josh@swigartlawgroup.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

V.

Defendant

Zillow Group, Inc.

represented by **Natalie Nola Peled**
Buchanan Ingersoll & Rooney
600 W. Broadway
Suite 1100
San Diego, CA 92101
619-239-8700
Fax: 619-702-3898
Email: natalie.peled@bipc.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
------------	---	-------------

09/15/2022	<u>1</u>	COMPLAINT with Jury Demand against Zillow Group, Inc. (Filing fee \$ 402 receipt number ACASDC-17167430.), filed by David Kauffman. (Attachments: # <u>1</u> Civil Cover Sheet) The new case number is 3:22-cv-1398-LL-AGS. Judge Linda Lopez and Magistrate Judge Andrew G. Schopler are assigned to the case. (Swigart, Joshua)(ggv) (sjt). (Entered: 09/15/2022)
09/15/2022	<u>2</u>	Summons Issued. Counsel receiving this notice electronically should print this summons and serve it in accordance with Rule 4, Fed.R.Civ.P and LR 4.1. (ggv) (sjt). (Entered: 09/15/2022)
09/27/2022	<u>3</u>	SUMMONS Returned Executed by David Kauffman. Zillow Group, Inc. served. (Shay, Daniel) (ddf). (Entered: 09/27/2022)
10/04/2022	<u>4</u>	Joint MOTION for Extension of Time to File Answer re <u>1</u> Complaint, by Zillow Group, Inc.. (Attachments: # <u>1</u> Proof of Service)(Peled, Natalie)Attorney Natalie Nola Peled added to party Zillow Group, Inc.(pty:dft) (ddf). (Entered: 10/04/2022)
10/06/2022	<u>5</u>	ORDER Granting Joint Motion To Extend Time To Answer Or Respond To Complaint [ECF No. <u>4</u>]. Signed by Judge Linda Lopez on 10/6/2022. (ddf) (Entered: 10/06/2022)

PACER Service Center			
Transaction Receipt			
10/19/2022 08:40:03			
PACER Login:	samanthasouthall	Client Code:	0106198-000001-SS
Description:	Docket Report	Search Criteria:	3:22-cv-01398-LL-AGS
Billable Pages:	2	Cost:	0.20

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS**

MARK CONLISK and MICHAEL
DEKHTYAR, individually and on behalf of
all others similarly situated,

Plaintiffs,

v.

ZILLOW GROUP, INC.,

Defendant.

Case No. _____

JURY TRIAL DEMANDED

COMPLAINT - CLASS ACTION

Plaintiffs Mark Conlisk and Michael Dekhtyar (“Plaintiffs”), individually and on behalf of all others similarly situated, hereby file this class action complaint against Defendant Zillow Group, Inc. (“Defendant” or “Zillow”), and in support thereof alleges the following:

INTRODUCTION

1. This is a class action brought against Zillow, the leading online homebuying marketplace, for surreptitiously intercepting the private electronic communications of visitors to its website, www.zillow.com, without their consent.

2. Zillow knowingly directs third-party vendors, such as Microsoft Corporation, to embed snippets of JavaScript computer code (“Session Replay Code”) on Zillow’s website, which then deploys on each website visitor’s internet browser for the purpose intercepting and recording the website visitor’s private electronic communications with the Zillow website, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time (“Website

Communications”). These third-party vendors (collectively, “Session Replay Providers”) create and deploy the Session Replay Code at Zillow’s request.

3. After intercepting and recording the Website Communications, Zillow and the Session Replay Providers use those Website Communications to recreate website visitors’ entire visit to www.zillow.com. The Session Replay Providers create a video replay of the user’s behavior on the website and provide it to Zillow for analysis. Zillow’s directive to the Session Replay Providers to secretly deploy the Session Replay Code results in the electronic equivalent of “looking over the shoulder” of each visitor to the Zillow website for the entire duration of their website interaction.

4. Zillow’s conduct violates the Illinois Eavesdropping Act, 720 ILCS 5/14-1, *et seq.*, the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.*, and constitutes an invasion of the privacy rights of website visitors.

5. Plaintiffs bring this action individually and on behalf of a class of all Illinois citizens whose Website Communications were intercepted at Zillow’s direction and use of Session Replay Code embedded on the webpages of www.zillow.com and seek all civil remedies provided under the causes of action, including but not limited to compensatory, statutory, and/or punitive damages, and attorneys’ fees and costs.

PARTIES

Plaintiff Mark Conlisk

6. Plaintiff Mark Conlisk is a citizen of the state of Illinois, and at all times relevant to this action, resided and was domiciled in Illinois. Plaintiff is a citizen of Illinois.

Plaintiff Michael Dekhtyar

7. Plaintiff Michael Dekhtyar is a citizen of the state of Illinois, and at all times relevant to this action, resided and was domiciled in Illinois. Plaintiff is a citizen of Illinois.

Defendant Zillow Group, Inc.

8. Defendant Zillow Group, Inc. is a corporation organized under the laws of Washington, and its principal place of business is located at 1301 Second Ave., Floor 31, Seattle Washington, 98101. Defendant is a citizen of Washington.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of \$5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class, including the Plaintiffs, who are citizens of a state (Illinois) different than Defendant (Washington).

10. This Court has personal jurisdiction over Defendant because a substantial part of the events and conduct giving rise to Plaintiffs' claims occurred in Illinois. The privacy violations complained of herein resulted from Defendant's purposeful and tortious acts directed towards citizens of Illinois while they were located within Illinois. At all relevant times, Defendant knew that its practices would directly result in collection of information from Illinois citizens while those citizens browse www.zillow.com. Defendant chose to avail itself of the business opportunities of making its real property and rental advertising services specifically available in Illinois (and specifically with respect to Illinois properties) and collecting real-time data from website visit sessions initiated by Illinoisans while located in Illinois, and the claims alleged herein arise from those activities.

11. Zillow also knows that many users visit and interact with Zillow’s websites while they are physically present in Illinois. Both desktop and mobile versions of Zillow’s website allow a user to search for nearby properties by providing the user’s “current location,” as furnished by the location-determining tools of the device the user is using or by the user’s IP address (*i.e.*, without requiring the user to manually input an address). Users’ employment of automatic location services in this way means that Zillow is continuously made aware that its website is being visited by people located in Illinois, and that such website visitors are being eavesdropped on in violation Illinois statutory and common law.

12. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

FACTUAL ALLEGATIONS

A. Website User and Usage Data Have Immense Economic Value.

13. The “world’s most valuable resource is no longer oil, but data.”¹

14. Earlier this year, Business News Daily reported that some businesses collect personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data (*i.e.*, how consumers interact with a business’s website, applications, and emails), behavioral data (*i.e.*, customers’ purchase histories and product usage information), and attitudinal data (*i.e.*, data on consumer satisfaction) from consumers.² This information is valuable to companies because

¹ *The world’s most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longeroil-but-data>.

² Max Freedman, *How Businesses Are Collecting Data (And What They’re Doing With It)*, Business News Daily (Aug. 5, 2022), <https://www.businessnewsdaily.com/10625-businesses-collecting-data.html>.

they can use this data to improve customer experiences, refine their marketing strategies, capture data to sell it, and even to secure more sensitive consumer data.³

15. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business's success. Research shows that organizations who "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."⁴

16. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."⁵ In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."⁶

17. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e. \$2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55."⁷

³ *Id.*

⁴ Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), <https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data>.

⁵ Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), <https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf>.

⁶ *Id.* at 25.

⁷ *Id.*

B. Website Users Have a Reasonable Expectation of Privacy in Their Interactions with Websites.

18. Consumers are skeptical and are wary about their data being collected. A report released by KPMG shows that “a full 86% of the respondents said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected.”⁸

19. Another recent paper also indicates that most website visitors will assume their detailed interactions with a website will only be used by the website and not be shared with a party they know nothing about.⁹ As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.¹⁰

20. Privacy polls and studies show that a majority of Americans consider one of the most important privacy rights to be the need for an individual’s affirmative consent before a company collects and shares its customers’ data.

21. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers’ data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.¹¹

⁸ Lance Whitney, *Data privacy is a growing concern for more consumers*, TechRepublic (Aug. 17, 2021), <https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/>.

⁹ *CUJO AI Recent Survey Reveals U.S. Internet Users Expectations and Concerns Towards Privacy and Online Tracking*, CUJO (May 26, 2020), <https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html>.

¹⁰ Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, The Information Society, 38:4, 257, 258 (2022).

¹¹ *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, Consumer Reports (May 11, 2017), <https://www.consumerreports.org/consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/>.

22. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.¹²

23. Users act consistently with their expectation of privacy. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.¹³

C. How Session Replay Code Works.

24. Session Replay Code, such as that implemented on www.zillow.com, enables website operators to record, save, and replay website visitors' interactions with a given website. The clandestinely deployed code provides online marketers and website designers with insights into the user experience by recording website visitors "as they click, scroll, type or navigate across different web pages."¹⁴

25. While Session Replay Code is utilized by websites for some legitimate purposes, it goes well beyond normal website analytics when it comes to collecting the actual contents of communications between website visitors and websites. Unlike other online advertising tools, Session Replay Code allows a website to capture and record nearly every action a website visitor takes while visiting the website, including actions that reveal the visitor's personal or private sensitive data, sometimes even when the visitor does not intend to submit the data to the website

¹² *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, (Nov. 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-Confusedand-feeling-lack-of-control-over-their-personal-information/>.

¹³ Margaret Taylor, *How Apple screwed Facebook*, Wired, (May 19, 2021), <https://www.wired.co.uk/article/apple-ios14-facebook>.

¹⁴ Erin Gilliam Haije, *[Updated] Are Session Recording Tools a Risk to Internet Privacy?*, Mopinion (Mar. 7, 2018), <https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/>.

operator, or has not finished submitting the data to the website operator.¹⁵ As a result, website visitors “aren’t just sharing data with the [web]site they’re on . . . but also with an analytics service that may be watching over their shoulder.”¹⁶

26. Session Replay Code works by inserting computer code into the various event handling routines that web browsers use to receive input from users, thus intercepting the occurrence of actions the user takes. When a website delivers Session Replay Code to a user’s browser, the browser will follow the code’s instructions by sending responses in the form of “event” data to a designated third-party server. Typically, the server receiving the event data is controlled by the third-party entity that wrote the Session Replay Code, rather than the owner of the website where the code is installed.

27. The types of events captured by Session Replay Code vary by specific product and configuration, but in general are wide-ranging and can encompass virtually every user action, including all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entry, and numerous other forms of a user’s navigation and interaction through the website. In order to permit a reconstruction of a user’s visit accurately, the Session Replay Code must be capable of capturing these events at hyper-frequent intervals, often just milliseconds apart. Events are typically accumulated and transmitted in blocks periodically throughout the user’s website session, rather than after the user’s visit to the website is completely finished.

28. Unless specifically masked through configurations chosen by the website owner, some visible contents of the website may also be transmitted to the Session Replay Provider.

¹⁵ *Id.*

¹⁶ Eric Ravenscraft, *Almost Every Website You Visit Records Exactly How Your Mouse Moves*, Medium (Feb. 5, 2020), <https://onezero.medium.com/almost-every-website-you-visit-records-exactly-how-your-mouse-moves-4134cb1cc7a0>.

29. Once the events from a user session have been recorded by a Session Replay Code, a website operator can view a visual reenactment of the user's visit through the Session Replay Provider, usually in the form of a video, meaning "[u]nlike typical analytics services that provide aggregate statistics, these scripts are intended for the recording and playback of individual browsing sessions."¹⁷

30. Because most Session Replay Codes will by default indiscriminately capture the maximum range of user-initiated events and content displayed by the website, researchers have found that a variety of highly sensitive information can be captured in event responses from website visitors, including medical conditions, credit card details, and other personal information displayed or entered on webpages.¹⁸

31. Most alarming, Session Replay Code may capture data that the user did not even intentionally transmit to a website during a visit, and then make that data available to website owners when they access the session replay through the Session Replay Provider. For example, if a user writes information into a text form field, but then chooses not to click a "submit" or "enter" button on the website, the Session Replay Code may nevertheless cause the non-submitted text to be sent to the designated event-response-receiving server before the user deletes the text or leaves the page. This information will then be viewable to the website owner when accessing the session replay through the Session Replay Provider.

32. Session Replay Code does not necessarily anonymize user sessions, either.

¹⁷ Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), <https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/>.

¹⁸ *Id.*

33. First, if a user’s entry of personally identifying information is captured in an event response, that data will become known and visible to both the Session Replay Provider and the website owner.

34. Second, if a website displays user account information to a logged-in user, that content may be captured by Session Replay Code.

35. Third, some Session Replay Providers explicitly offer website owners cookie functionality that permits linking a session to an identified user, who may be personally identified if the website owner has associated the user with an email address or username.¹⁹

36. Session Replay Providers often create “fingerprints” that are unique to a particular user’s combination of computer and browser settings, screen configuration, and other detectable information. The resulting fingerprint, which is often unique to a user and rarely changes, are collected across all sites that the Session Replay Provider monitors.

37. When a user eventually identifies themselves to one of these websites (such as by filling in a form), the provider can then associate the fingerprint with the user identity and can then back-reference all of that user’s other web browsing across other websites previously visited, including on websites where the user had intended to remain anonymous—even if the user explicitly indicated that they would like to remain anonymous by enabling private browsing.

38. In addition to the privacy invasions caused by the diversion of user communications with websites to third-party Session Replay Providers, Session Replay Code also exposes website visitors to identity theft, online scams, and other privacy threats.²⁰ Indeed, “[t]he more copies of

¹⁹ *Id.*; see also *FS.identify – Identifying users*, FullStory, <https://help.fullstory.com/hc/en-us/articles/360020828113>, (last visited Sep. 8, 2022).

²⁰ Juha Sarrinen, *Session Replay is a Major Threat to Privacy on the Web*, itnews (Nov. 16, 2017), <https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720>.

sensitive information that exist, the broader the attack surface, and when data is being collected [] it may not be stored properly or have standard protections” increasing “the overall risk that data will someday publicly leak or be breached.”²¹

39. Recognizing the privacy concerns posed by Session Replay Code, in 2019 Apple required app developers to remove or properly disclose the use of analytics code that allow app developers to record how a user interacts with their iPhone apps or face immediate removal from the app store.²² In announcing this decision, Apple stated: “Protecting user privacy is paramount in the Apple ecosystem. Our App Store Review Guidelines require that apps request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity.”²³

D. Zillow Secretly Eavesdrops on its Website Visitors’ Electronic Communications.

40. Zillow operates the website www.zillow.com. Zillow is the “leading online residential real estate” marketplace in the United States for consumers, connecting them to the information and real estate professionals they need to buy, sell, or rent a home.²⁴

41. Zillow has become “synonymous with residential real estate.”²⁵ www.zillow.com is the most popular real estate website in the United States, with over thirty-six million unique

²¹ Lily Hay Newman, *Covert ‘Replay Sessions’ Have Been harvesting Passwords by Mistake*, WIRED (Feb. 26, 2018), <https://www.wired.com/story/covert-replay-sessions-harvesting-passwords/>.

²² Zack Whittaker, *Apple Tells App Developers to Disclose or Remove Screen Recording Code*, TechCrunch (Feb. 7, 2019), <https://techcrunch.com/2019/02/07/apple-glassbox-apps/>.

²³ *Id.*

²⁴ Zillow Group, Inc., *Form 10-K* (Dec. 31, 2021), <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001617640/87bbb30-39cb-4eb7-acdc-1b51265b9687.pdf> (“Zillow 10-K”).

²⁵ *Id.*

monthly visitors²⁶ and more than 135 million properties are listed on its website.²⁷ According to a 2021 Google Trends report, “[t]oday more people search ‘Zillow’ than ‘real estate.’”²⁸

42. However, unbeknownst to the millions of individuals perusing Zillow’s real estate listings, Zillow knowingly directs Session Replay Providers to embed various Session Replay Codes on its website to track and analyze website user interactions with www.zillow.com. Because the Session Replay Providers are unknown eavesdroppers to visitors to www.zillow.com, they are not parties to website visitors’ Website Communications with Zillow.

43. One such Session Replay Provider that Zillow procures is Microsoft.

44. Microsoft is the owner and operator of a Session Replay Code titled Clarity, which provides basic information about website user sessions, interactions, and engagement, and breaks down users by device type, county, and other dimensions.²⁹

45. Zillow knowingly derives a benefit and/or information from the Website Communications intercepted and recorded at its direction. Upon information and belief, Zillow uses the intercepted Website Communications to replay website visitors’ interactions with www.zillow.com, improve user interactions with its website, and to provide targeted real estate advertisements to its website visitors.

46. Zillow’s knowing direction and use of Microsoft Clarity’s Session Replay Code, direction and use of other Session Replay Codes through various Session Replay Providers, and its knowing derivation of a benefit and/or information from the Website Communications

²⁶ *Most Popular Real Estate Websites in the United States as of October 2021, Based on Unique Monthly Visits*, Statista, <https://www.statista.com/statistics/381468/most-popular-real-estate-websites-by-monthly-visits-usa/>, (last visited Sep. 8, 2022).

²⁷ Zillow 10-K, *supra*, note 1.

²⁸ *Id.*

²⁹ Jono Alderson, *An Introduction to Microsoft Clarity*, Yoast, <https://yoast.com/introduction-microsoft-clarity/#h-what-is-microsoft-clarity>, (last visited Sep. 8, 2022).

surreptitiously intercepted and recorded by Session Replay Codes is a violation of Illinois statutory and common law.

E. Plaintiffs' and Class Members' Experiences.

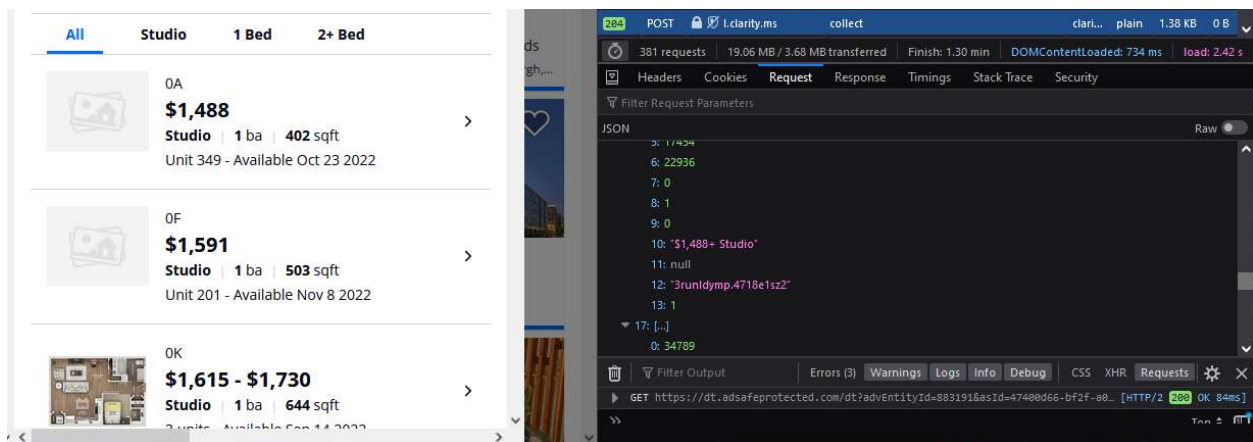
47. Plaintiffs have each independently visited www.zillow.com on his device while in Illinois on at least one occasion.

48. While visiting Zillow's website, Plaintiffs fell victim to Defendant's unlawful monitoring, recording, and collection of Plaintiffs' Website Communications with www.zillow.com.

49. Unknown to Plaintiffs, Zillow directs Session Replay Providers to embed Session Replay Code on its website.

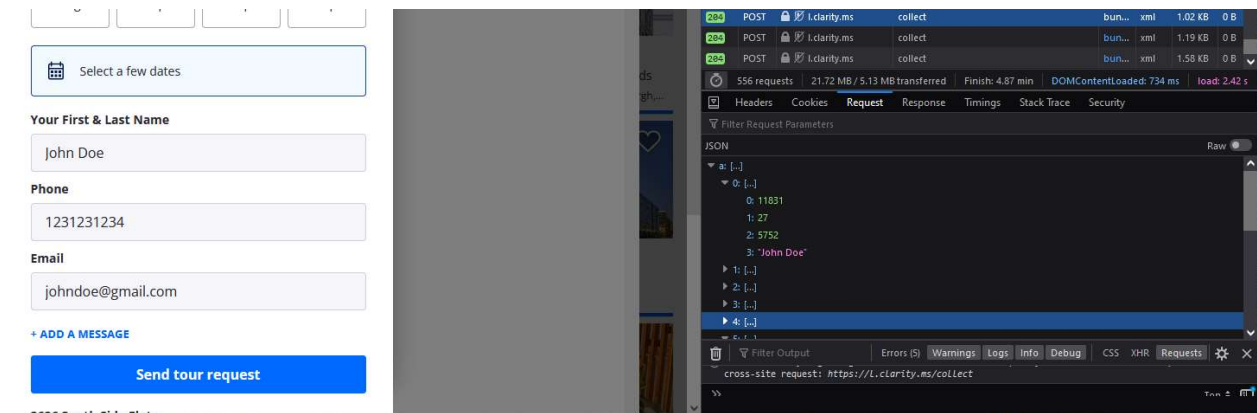
50. During the website visit(s), Plaintiffs' Website Communications were captured by Session Replay Code and sent to various Session Replay Providers.

51. For example, when visiting www.zillow.com, if a website user views a certain piece of property for rent or sale, that information is captured by the Session Replay Codes embedded on the website:



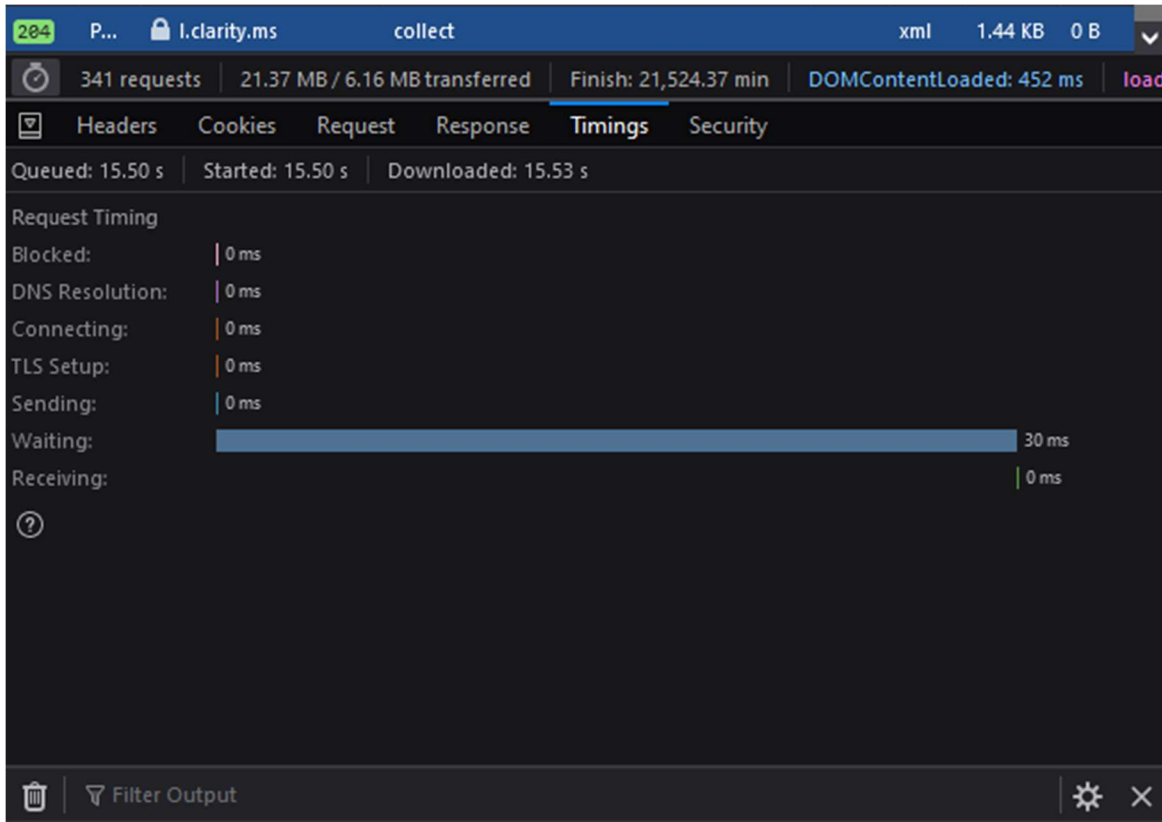
Depicting information sent to one of the Service Replay Providers—Microsoft—through a Service Replay Code—Clarity—after viewing a Studio apartment priced at \$1,488 while visiting www.zillow.com.

52. Similarly, when visiting www.zillow.com, if a user enters personal information in a text box to schedule a tour, that information is captured by the Session Replay Codes embedded on the website:



Depicting information sent to one of the Service Replay Providers—Microsoft—through a Service Replay Code—Clarity—after entering a name (purple text) to a text box to schedule a tour of a property.

53. The eavesdropping by the Session Replay Code is ongoing during the visit and they intercept the contents of these communications between Plaintiffs and Zillow with instantaneous transmissions to the Session Replay Providers, as illustrated below, in which only 30 milliseconds were required to send a packet of even response data, which would indicate whatever the website user had just done:



54. The Session Replay Codes operate in the same manner for all putative Class members.

55. Like Plaintiffs, each Class member visited www.zillow.com with Session Replay Code embedded in it, and those Session Replay Codes intercepted the Class members' Website Communications with www.zillow.com by sending hyper-frequent logs of those communications to Session Replay Providers.

56. Even if Zillow masks certain elements when it configures the settings of the Session Replay Code embedded on its website, any operational iteration of the Session Replay Code will, by its very nature and purpose, intercept the contents of communications between the website's visitors and the website owner.

57. For example, even with heightened masking enabled, Session Replay Providers will still learn through the intercepted data exactly which pages a user navigates to, how the user moves

through the page (such as which areas the user zooms in on or interacted with), and additional substantive information.

58. As a specific example, if a user types a particular address or zip code into Zillow's main search bar and initiates a search, even if the text entered into the search bar is masked, Session Replay Providers will still learn what is entered into the bar as soon as the search result page loads. This is so because the responsive search results will be displayed on the subsequent page, and the responsive content generated by Zillow will repeat the searched information back on the generated page. That information will not be masked even if user-inputted text is fully masked in a text field.

CLASS ACTION ALLEGATIONS

59. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Class:

All natural persons in the State of Illinois whose Website Communications were captured through the use of Session Replay Code embedded in www.zillow.com.

60. Excluded from the class are Defendant, its parents, subsidiaries, affiliates, officers, and directors, all persons who make a timely election to be excluded from the class, the judge to whom this case is assigned and any immediate family members thereof, and the attorneys who enter their appearance in this action.

61. **Numerosity:** The members of the Class are so numerous that individual joinder of all Class members is impracticable. The precise number of Class members and their identities may be obtained from the books and records of Zillow or the Session Replay Providers.

62. **Commonality:** This action involves questions of law and fact that are common to the Class members. Such common questions include, but are not limited to: (a) whether Defendant employed Session Replay Providers to intercept and record Zillow's website visitors' Website Communications; (b) whether Defendant operated or participated in the operation of an

eavesdropping device; (c) whether Defendant derives a benefit or information from the illegal use of an eavesdropping device; (d) whether Defendant directed another to use an eavesdropping device illegally on its behalf; (e) whether Session Replay Code is an “eavesdropping device” used to intercept or record private electronic communications; (f) whether Defendant acquired the contents of website users’ private electronic communications without their consent; (g) whether Plaintiffs and Class members had a reasonable expectation of privacy in their Website communications; (f) whether Defendant violated the Illinois Eavesdropping Act 720 ILCS 5/14-1, *et seq.*; (g) whether Defendant’s interception of Plaintiffs’ and Class members’ private electronic communications is an unfair or deceptive act or practice; (h) whether Zillow’s conduct violates the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.* (i) whether Plaintiffs and the Class members are entitled to equitable relief; and (j) whether Plaintiffs and the Class members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

63. **Typicality:** Plaintiffs’ claims are typical of the other Class members’ claims because, among other things, all Class members were comparably injured through the uniform prohibited conduct described above. For instance, Plaintiffs and each member of the Class had their electronic communications intercepted in violation of the law and their right to privacy. This uniform injury and the legal theories that underpin recovery make the claims of Plaintiffs and the members of the Class typical of one another.

64. **Adequacy of Representation:** Plaintiffs have and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiffs have retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiffs have no interest that is antagonistic to the interests of the Class, and

Defendant has no defenses unique to any Plaintiff(s). Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to the interests of the other members of the Class.

65. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

66. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiffs and each member of the Class. If Defendant intercepted Plaintiffs' and Class members' Website Communications, then Plaintiffs and each Class member suffered damages by that conduct.

67. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class members may be readily identified through Zillow's books and records or the Session Replay Providers' books and records.

COUNT I
Violation of Illinois Eavesdropping Act
720 ILCS 5/14-1, *et seq.*

68. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

69. Plaintiffs bring this claim individually and on behalf of the Class.

70. The Illinois Eavesdropping Act (the “Act”) prohibits (1) using an eavesdropping device in a surreptitious manner to overhear, transmit, or record all or any part of any private conversation; (2) intercepting, recording, or transcribing, in a surreptitious manner, any private electronic communication without consent; (3) manufacturing, assembling, distributing, or possessing any electronic, mechanical, eavesdropping, or other device knowing that or having reason to know that the design of the device renders it primarily useful for the purpose of surreptitious overhearing, transmitting, or recording of private conversations or the intersection; or (4) using or disclosing any information which he or she knows or reasonably should know was obtained from a private conversation or private electronic communication without the consent of all parties to the private electronic communication. 720 ILCS 5/14-2.

71. Any party to any conversation or private electronic communication upon which eavesdropping was practiced shall be entitled to (1) an injunction to prohibit further eavesdropping; (2) actual damages; and (3) punitive damages. punitive damages; 720 ILCS 5/14-6.

72. “Eavesdropping device” is defined as any “any device capable of being used to hear or record oral conversation or intercept, or transcribe electronic communications whether such conversation or electronic communication is conducted in person, by telephone, or by any other means[.]” 720 ILCS 5/14-1(a).

73. “Eavesdropper” is defined as “any person, including any law enforcement officer and any party to a private conversation, who operates or participates in the operation of any eavesdropping device contrary to the provisions of this Article or who acts as a principal, as defined in this Article.” 720 ILCS 5/14-1(b).

74. “Principle” is defined as “any person who: (1) knowingly employs another who illegally uses an eavesdropping device in the course of such employment; or (2) knowingly derives any benefit or information from the illegal use of an eavesdropping device by another; or (3) directs another to use an eavesdropping device illegally on his or her behalf.” 720 ILCS 5/14-1(c).

75. “Private electronic communication” is defined as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation. A reasonable expectation shall include any expectation recognized by law, including, but not limited to, an expectation derived from a privilege, immunity, or right established by common law, Supreme Court rule, or the Illinois or United States Constitution.” ILCS 5/14-1(e).

76. “Surreptitious” is defined as being “obtained or made by stealth or deception, or executed through secrecy or concealment.” 720 ILCS 5/14-1(g).

77. Zillow is an “Eavesdropper” and “Principal” for purposes of the Act because it operates or participates in the operation of an eavesdropping device, knowingly employs another who illegally uses an eavesdropping device, derives a benefit or information from the illegal use of an eavesdropping device, and directs another to use an eavesdropping device illegally on its behalf.

78. Session Replay Code like that operated and employed at Zillow’s direction is a “eavesdropping device” used to transcribe electronic communications within the meaning of the Act.

79. The Session Replay Providers are not a party to the Website Communications—Plaintiffs and the Class only knew they were communicating with Zillow, not the Session Replay Providers.

80. Plaintiffs’ and Class members’ intercepted Website Communications constitute the private electronic communications and private conversations within the meaning of the Act.

81. Zillow intentionally operated and employed Session Replay Code on its website to spy on, automatically and secretly, and intercept its website visitors’ private electronic interactions communications with Zillow in real time.

82. Plaintiffs’ and Class members’ private electronic communications were intercepted contemporaneously with their transmission.

83. Plaintiffs and Class members had a reasonable expectation of privacy in their Website Communications based on the detailed information the Session Replay Code collected from Plaintiffs and Class members.

84. Plaintiffs and Class members did not consent to having their Website Communications surreptitiously intercepted and recorded.

85. Pursuant to 720 ILCS 5/14-6, Plaintiff and members of the Class are entitled to: (1) an injunction to prohibit further eavesdropping; (2) actual damages; and (3) punitive damages.

86. Zillow’s conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiffs and Class members any time they visit Defendant’s website with Session Replay Code enabled without their consent. Plaintiffs and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT II

**Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act
815 ILCS 505/1 *et seq.***

87. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

88. Plaintiffs bring this claim individually and on behalf of the Class.

89. The Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.* (“ICFA”) protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

90. The ICFA prohibits “unfair or deceptive acts or practices,” including “misrepresentation or the concealment, suppression or omission of any material fact.” 815 ILCS 505/2.

91. The ICFA applies to Zillow’s conduct described herein because it protects consumers in transactions that are intended to result, or which have resulted in the sale of goods or services.

92. Zillow is a “person” within the meaning of ILCS 505/1(c) because it is a corporation.

93. Plaintiffs and members of the Class are “consumers” within the meaning of 815 ILCS 505/1(e) because they visited www.zillow.com to shop for, purchase, or contract to purchase “merchandise”—real estate—for their own use.

94. Zillow’s advertising, offering for sale, and sale of real estate on www.zillow.com is considered “trade” or “commerce” within the meaning of 815 ILCS 505/1(f).

95. Zillow violated the ICFA by concealing material facts about www.zillow.com. Specifically, Zillow omitted and concealed that it directed Session Replay Providers to secretly

monitor, collect, transmit, and discloses its website visitors' Website Communications to the Session Replay Providers using Session Replay Code.

96. Zillow's direction and employment of the Session Replay Providers and their Session Replay Codes to intercept, collect, and disclose website visitors' Website Communications are material to the transactions on www.zillow.com. Zillow is leading online residential real estate marketplace in the United States and Zillow does not disclose its use of Session Replay Code to secretly monitor and collect website visitors' Website Communications. Had Plaintiffs and the Class members known that the Session Replay Codes (that collect, transmit, and disclose Website Communications to the Session Replay Providers) were embedded in Zillow's website, they would not have visited www.zillow.com to shop for, purchase, or contract to purchase real estate or they would have required Zillow to compensate them for the interception, collection, and disclosure of their Website Communications.

97. Zillow's intentionally concealed the interception, collection, and disclosure of website visitors' Website Communications using Session Replay Code embedded in www.zillow.com is material because it knows that consumers would not otherwise visit its website to search for, purchase, and contract to purchase real estate. Indeed, Zillow's concealment of such facts was intended to mislead consumers.

98. Zillow's concealment, suppression, and omission of material facts was likely to mislead reasonable consumers under the circumstances, and thus constitutes an unfair and deceptive trade practice in violation of the ICFA.

99. By failing to disclose and inform Plaintiffs and the Class about its interception, collection, and disclosure of website visitors' Website Communications, Zillow violated section 505/2 of the ICFA.

100. As a direct and proximate result of these unfair and deceptive practices, Plaintiffs and each Class member has suffered actual harm in the form of money and/or property because the disclosure of their Website Communications has value as demonstrated by the collection and use of it by Zillow. The collection and use of this information has now diminished the value of such information to Plaintiffs and the Class.

101. As such, Plaintiffs and the Class seek an order (1) requiring Zillow to cease the unfair practices described herein; (2) awarding actual damages; and (3) awarding reasonable attorneys' fees and costs.

102. Zillow's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiffs and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT III
Invasion of Privacy – Intrusion Upon Seclusion

103. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

104. Plaintiffs bring this claim individually and on behalf of the Class.

105. Illinois common law recognizes the tort of invasion of privacy. The right to privacy is also embodied in the Illinois constitution.

106. Plaintiffs and Class members had an objective, reasonable expectation of privacy in their Website Communications.

107. Plaintiffs and Class members did not consent to, authorize, or know about Zillow's intrusion at the time it occurred. Plaintiffs and Class members never agreed that Zillow could collect or disclose their Website Communications.

108. Plaintiffs and Class members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

109. Zillow intentionally intruded on Plaintiffs' and Class members' private life, seclusion, or solitude, without consent.

110. Zillow's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

111. Plaintiffs and Class members were harmed by Zillow's wrongful conduct as Zillow's conduct has caused Plaintiffs and the Class mental anguish and suffering arising from their loss of privacy and confidentiality of their electronic communications.

112. Zillow's conduct has needlessly harmed Plaintiffs and the Class by capturing intimately personal facts and data in the form of their Website Communications. This disclosure and loss of privacy and confidentiality has caused Plaintiffs and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

113. Additionally, given the monetary value of individual personal information, Defendant deprived Plaintiffs and Class members of the economic value of their interactions with Defendant's website, without providing proper consideration for Plaintiffs' and Class members' property.

114. Further, Zillow has improperly profited from its invasion of Plaintiffs and Class members' privacy in its use of their data for its economic value.

115. As a direct and proximate result Zillow's conduct, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

116. Zillow's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiffs and Class members any time they visit Defendant's website with session replay software enabled without their consent. Plaintiffs and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

REQUEST FOR RELIEF

Plaintiffs, individually and on behalf of the other members of the proposed Class, respectfully requests that the Court enter judgment in Plaintiffs' and the Class's favor and against Defendant as follows:

- A. Certifying the Class and appointing Plaintiffs as the Class representatives;
- B. Appointing Plaintiffs' counsel as class counsel;
- C. Declaring that Defendant's past conduct was unlawful, as alleged herein;
- D. Declaring Defendant's ongoing conduct is unlawful, as alleged herein;
- E. Enjoining Defendant from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;
- F. Awarding Plaintiffs and the Class members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;
- G. Awarding Plaintiffs and the Class members pre-judgment and post-judgment interest;

H. Awarding Plaintiffs and the Class members reasonable attorneys' fees, costs, and expenses; and

I. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the Class, demands a trial by jury of any and all issues in this action so triable of right.

DATED: September 19, 2022

Respectfully Submitted,

s/ Gary M. Klinger

Gary M. Klinger

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC

227 W. Monroe Street, Suite 2100

Chicago, IL 60606

Phone: 866.252.0878

gklinger@milberg.com

Nick Suciu III

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC

6905 Telegraph Road, Suite 115

Bloomfield Hills, MI 48301

Tel: (313) 303-3472

nsuciu@milberg.com

[Query](#) [Reports](#) [Utilities](#) [Help](#) [Log Out](#)

FINNEGAN

**United States District Court
Northern District of Illinois - CM/ECF NextGen 1.6.3 (Chicago)
CIVIL DOCKET FOR CASE #: 1:22-cv-05082**

Conlisk et al v. Zillow Group, Inc.
Assigned to: Honorable John F. Kness
Demand: \$75,000
Cause: 28:1332 Diversity-Personal Injury

Date Filed: 09/19/2022
Jury Demand: Plaintiff
Nature of Suit: 360 P.I.: Other
Jurisdiction: Diversity

Plaintiff

Mark Conlisk
*individually and on behalf of all others
similarly situated*

represented by **Gary M. Klinger**
Milberg Coleman Bryson Phillips Grossman
PLLC
227 W. Monroe Street
Suite 2100
Chicago, IL 60606
866-252-0878
Email: gklinger@milberg.com
ATTORNEY TO BE NOTICED

Plaintiff

Michael Dekhtyar
*individually and on behalf of all others
similarly situated*

represented by **Gary M. Klinger**
(See above for address)
ATTORNEY TO BE NOTICED

V.

Defendant

Zillow Group, Inc.

represented by **David T Cellitti**
Buchanan Ingersoll & Rooney PC
401 E. Jackson Street, Suite 2400
Tampa, FL 33602-5236
(813) 222-1137
Fax: Not a member
Email: david.cellitti@bipc.com
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
09/19/2022	1	COMPLAINT - <i>Class Action</i> filed by Mark Conlisk, Michael Dekhtyar; Jury Demand. Filing fee \$ 402, receipt number AILNDC-19853896. (Attachments: # 1 Civil Cover Sheet) (Klinger, Gary) (Entered: 09/19/2022)
09/19/2022		CASE ASSIGNED to the Honorable John F. Kness. Designated as Magistrate Judge the Honorable Sheila M. Finnegan. Case assignment: Random assignment. (mbh,) (Entered: 09/19/2022)

09/19/2022		CLERK'S NOTICE: Pursuant to Local Rule 73.1(b), a United States Magistrate Judge of this court is available to conduct all proceedings in this civil action. If all parties consent to have the currently assigned United States Magistrate Judge conduct all proceedings in this case, including trial, the entry of final judgment, and all post-trial proceedings, all parties must sign their names on the attached Consent To form. This consent form is eligible for filing only if executed by all parties. The parties can also express their consent to jurisdiction by a magistrate judge in any joint filing, including the Joint Initial Status Report or proposed Case Management Order. (mbh,) (Entered: 09/19/2022)
09/19/2022		SUMMONS Issued as to Defendant Zillow Group, Inc. (jk2,) (Entered: 09/19/2022)
10/11/2022	2	ATTORNEY Appearance for Defendant Zillow Group, Inc. by David T Cellitti (Cellitti, David) (Entered: 10/11/2022)
10/11/2022	3	MOTION by Defendant Zillow Group, Inc. for extension of time to file answer <i>move or otherwise respond to Plaintiffs' Complaint</i> (Cellitti, David) (Entered: 10/11/2022)
10/12/2022	4	MINUTE entry before the Honorable John F. Kness: Defendant's Motion for extension of time to answer 3 is granted. Defendant must answer on otherwise plead to Plaintiff's complaint on or before 12/12/2022. Status hearing set for 12/21/2022 at 09:30 AM. Consistent with Rule 26(f) of the Federal Rules of Civil Procedure, the parties are directed to meet and conduct a planning conference in advance of the initial status hearing. No later than seven days before the status hearing, the parties shall jointly complete and file on the docket a report that provides the information required by the Court's model Joint Initial Status Report, which can be found at https://www.ilnd.uscourts.gov/judge-info.aspx?Iu9/vqz23r5X7AkWx/nLtg== (see link entitled "Joint Initial Status Report"). If all Defendants have not yet been served or have not yet responded to requests to draft the required Joint Initial Status Report, Plaintiff must file the report on its own and must inform the Court of that circumstance. The parties are to use the following call-in number: 888-684-8852, conference code 3796759. The public and media representatives may have access to the hearing via the same number. Audio recording of the hearing is not permitted; violations of this prohibition may result in sanctions. Participants are directed to keep their device muted when they are not speaking. Mailed notice (ef,) (Entered: 10/12/2022)

PACER Service Center			
Transaction Receipt			
10/19/2022 10:41:17			
PACER Login:	samanthasouthall	Client Code:	0106198-000001-SS
Description:	Docket Report	Search Criteria:	1:22-cv-05082
Billable Pages:	2	Cost:	0.20

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

NATALIE PERKINS and KENNETH
HASSON, individually and on behalf themselves
and of all others similarly situated,

Plaintiffs,

v.

ZILLOW GROUP, INC. and MICROSOFT
CORPORATION,

Defendants.

NO.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Natalie Perkins and Kenneth Hasson (“Plaintiffs”), individually and on behalf of themselves and all others similarly situated, hereby file this class action complaint against Defendant Zillow Group, Inc. (“Zillow”) and Defendant Microsoft Corporation (“Microsoft”) (collectively “Defendants”), and in support thereof alleges the following:

INTRODUCTION

1. This is a class action brought against Defendants for wiretapping the electronic communications of visitors to Zillow’s website, www.zillow.com (“Zillow’s website”). Zillow procures third-party vendors, such as Microsoft Corporation, to embed snippets of JavaScript computer code (“Session Replay Code”) on Zillow’s website, which then deploys on each

1 website visitor’s internet browser for the purpose intercepting and recording the website
2 visitor’s electronic communications with the Zillow website, including their mouse movements,
3 clicks, keystrokes (such as text being entered into an information field or text box), URLs of
4 web pages visited, and/or other electronic communications in real-time (“Website
5 Communications”). These third-party vendors (collectively, “Session Replay Providers”)
6 create and deploy the Session Replay Code at Zillow’s request.

7 2. After intercepting and capturing the Website Communications, Zillow,
8 Microsoft and other Session Replay Providers use those Website Communications to recreate
9 website visitors’ entire visit to Zillow’s website. Microsoft and other Session Replay Providers
10 create a video replay of the user’s behavior on the website and provide it to Zillow for analysis.
11 Zillow’s procurement of the Session Replay Providers to secretly deploy the Session Replay
12 Code results in the electronic equivalent of “looking over the shoulder” of each visitor to the
13 Zillow website for the entire duration of their website interaction.

14 3. Defendants’ conduct violates the Washington Wiretapping Statute, Wash. Rev.
15 Code §9.73.030 *et seq.* and constitutes an invasion of the privacy rights of website visitors.

16 4. Plaintiffs bring this action individually and on behalf of a nationwide class of all
17 individuals whose Website Communications were intercepted through Defendants’
18 procurement and use of Session Replay Code embedded on the webpages of Zillow’s website
19 and seeks all civil remedies provided under the causes of action, including but not limited to
20 compensatory, statutory, and/or punitive damages, and attorneys’ fees and costs.

21 **PARTIES**

22 5. Plaintiff Natalie Perkins is a citizen of South Carolina and at all times relevant to
23 this action, resided and was domiciled in York County, South Carolina.

6. Plaintiff Kenneth Hasson is a citizen of Pennsylvania, and at all times relevant to this action, resided and was domiciled in Lawrence County, Pennsylvania

7. Defendant Zillow Group, Inc. is corporation organized under the laws of Washington, and its principal place of business is located at 1301 Second Ave., Floor 31, Seattle, Washington, 98101. Defendant is a citizen of Washington.

8. Defendant Microsoft Inc. is a corporation organized under the laws of Washington, and its principal place of business is located at One Microsoft Way, Redmond, Washington, 98052. Defendant is a citizen of Washington.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of \$5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class, including Plaintiffs, are citizens of a state different than Defendants.

10. This Court has personal jurisdiction over Defendants because a substantial part of the events and conduct giving rise to Plaintiffs' claims occurred in the state of Washington. The privacy violations complained of herein resulted from Defendants' purposeful and tortious acts directed towards citizens throughout the United States. Additionally, Zillow's Terms of Use specifically state that individuals' Terms of Use are governed by the laws of the State of Washington, without giving effect to its conflict of laws' provisions, and that Defendant Zillow operates the services it provides to individuals from Zillow's offices in the State of Washington. See <https://www.zillowgroup.com/terms-of-use/>.

11. At all relevant times, Defendants knew that their practices would directly result in collection of information throughout the United States while individuals browse Zillow’s website. Defendants chose to avail themselves of the business opportunities of making Zillow’s real property and rental advertising services specifically available through Washington and collecting real-time data from website visit sessions initiated by individuals located throughout the United States, including in Washington, and the claims alleged herein arise from those activities.

12. Zillow also knows that many users visit and interact with Zillow’s websites while they are physically present in Washington and throughout the United States. Both desktop and mobile versions of Zillow’s website allow a user to search for nearby properties by providing the user’s “current location,” as furnished by the location-determining tools of the device the user is using or by the user’s IP address (*i.e.*, without requiring the user to manually input an address). Users’ employment of automatic location services in this way means that Zillow is continuously made aware that its website is being visited by people located throughout the United States, including in Washington, and that such website visitors are being wiretapped in violation Washington statutory and common law.

13. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

FACTUAL ALLEGATIONS

A. Website User and Usage Data Have Immense Economic Value.

14. The “world’s most valuable resource is no longer oil, but data.”¹

15. Earlier this year, Business News Daily reported that some businesses collect personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data (*i.e.*, how consumers interact with a business’s website, applications, and emails), behavioral data (*i.e.*, customers’ purchase histories and product usage information), and attitudinal data (*i.e.*, data on consumer satisfaction) from consumers.² This information is valuable to companies because they can use this data to improve customer experiences, refine their marketing strategies, capture data to sell it, and even to secure more sensitive consumer data.³

16. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business’s success. Research shows that organizations who “leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin.”⁴

17. In 2013, the Organization for Economic Cooperation and Development (“OECD”) even published a paper entitled “Exploring the Economics of Personal Data: A

¹ *The world’s most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longeroil-but-data>.

² Max Freedman, *How Businesses Are Collecting Data (And What They’re Doing With It)*, Business News Daily (Aug. 5, 2022), <https://www.businessnewsdaily.com/10625-businesses-collecting-data.html>.

³ *Id.*

⁴ Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), <https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data>.

Survey of Methodologies for Measuring Monetary Value.”⁵ In this paper, the OECD measured prices demanded by companies concerning user data derived from “various online data warehouses.”⁶

18. OECD indicated that “[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e. \$2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver’s license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55.”⁷

B. Website Users Have a Reasonable Expectation of Privacy in Their Interactions with Websites.

19. Consumers are skeptical and are wary about their data being collected. A report released by KPMG shows that “a full 86% of the respondents said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected.”⁸

20. Another recent paper also indicates that most website visitors will assume their detailed interactions with a website will only be used by the website and not be shared with a party they know nothing about.⁹ As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.¹⁰

⁵ Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), <https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf>.

⁶ *Id.* at 25.

⁷ *Id.*

⁸ Lance Whitney, *Data privacy is a growing concern for more consumers*, TechRepublic (Aug. 17, 2021), <https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/>.

⁹ *CUJO AI Recent Survey Reveals U.S. Internet Users Expectations and Concerns Towards Privacy and Online Tracking*, CUJO (May 26, 2020), <https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html>.

¹⁰ Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, *The Information Society*, 38:4, 257, 258 (2022).

21. Privacy polls and studies show that a majority of Americans consider one of the most important privacy rights to be the need for an individual’s affirmative consent before a company collects and shares its customers’ data.

22. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers’ data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.¹¹

23. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.¹²

24. Users act consistently with their expectation of privacy. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.¹³

C. How Session Replay Code Works.

25. Session Replay Code, such as that implemented on Zillow’s website, enables website operators to record, save, and replay website visitors’ interactions with a given website.

¹¹ *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, Consumer Reports (May 11, 2017), <https://www.consumerreports.org/consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/>.

¹² *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, (Nov. 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-Confusedand-feeling-lack-of-control-over-their-personal-information/>.

¹³ Margaret Taylor, *How Apple screwed Facebook*, Wired, (May 19, 2021), <https://www.wired.co.uk/article/apple-ios14-facebook>.

1 The clandestinely deployed code provides online marketers and website designers with insights
2 into the user experience by recording website visitors “as they click, scroll, type or navigate
3 across different web pages.”¹⁴

4 26. While Session Replay Code is utilized by websites for some legitimate purposes,
5 it goes well beyond normal website analytics when it comes to collecting the actual contents of
6 communications between website visitors and websites. Unlike other online advertising tools,
7 Session Replay Code allows a website to capture and record nearly every action a website
8 visitor takes while visiting the website, including actions that reveal the visitor’s personal or
9 private sensitive data, sometimes even when the visitor does not intend to submit the data to the
10 website operator, or has not finished submitting the data to the website operator.¹⁵ As a result,
11 website visitors “aren’t just sharing data with the [web]site they’re on . . . but also with an
12 analytics service that may be watching over their shoulder.”¹⁶

13 27. Session Replay Code works by inserting computer code into the various event
14 handling routines that web browsers use to receive input from users, thus intercepting the
15 occurrence of actions the user takes. When a website delivers Session Replay Code to a user’s
16 browser, the browser will follow the code’s instructions by sending responses in the form of
17 “event” data to a designated third-party server. Typically, the server receiving the event data is
18 controlled by the third-party entity that wrote the Session Replay Code, rather than the owner
19 of the website where the code is installed.

21 ¹⁴ Erin Gilliam Haije, *[Updated] Are Session Recording Tools a Risk to Internet Privacy?*, Mopinion
22 (Mar. 7, 2018), <https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/>.

23 ¹⁵ *Id.*

¹⁶ Eric Ravenscraft, *Almost Every Website You Visit Records Exactly How Your Mouse Moves*, Medium
(Feb. 5, 2020), <https://onezero.medium.com/almost-every-website-you-visit-records-exactly-how-your-mouse-moves-4134cb1cc7a0>.

28. The types of events captured by Session Replay Code vary by specific product and configuration, but in general are wide-ranging and can encompass virtually every user action, including all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entry, and numerous other forms of a user’s navigation and interaction through the website. To permit a reconstruction of a user’s visit accurately, the Session Replay Code must be capable of capturing these events at hyper-frequent intervals, often just milliseconds apart. Events are typically accumulated and transmitted in blocks periodically throughout the user’s website session, rather than after the user’s visit to the website is completely finished.

29. Unless specifically masked through configurations chosen by the website owner, some visible contents of the website may also be transmitted to the Session Replay Provider.

30. Once the events from a user session have been recorded by a Session Replay Code, a website operator can view a visual reenactment of the user’s visit through the Session Replay Provider, usually in the form of a video, meaning that “[u]nlike typical analytics services that provide aggregate statistics, these scripts are intended for the recording and playback of individual browsing sessions.”¹⁷

31. Because most Session Replay Codes will by default indiscriminately capture the maximum range of user-initiated events and content displayed by the website, researchers have found that a variety of highly sensitive information can be captured in event responses from website visitors, including medical conditions, credit card details, and other personal information displayed or entered on webpages.¹⁸

¹⁷ Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), <https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/>.

¹⁸ *Id.*

32. Most alarming, Session Replay Code may capture data that the user did not even intentionally transmit to a website during a visit, and then make that data available to website owners when they access the session replay through the Session Replay Provider. For example, if a user writes information into a text form field, but then chooses not to click a “submit” or “enter” button on the website, the Session Replay Code may nevertheless cause the non-submitted text to be sent to the designated event-response-receiving server before the user deletes the text or leaves the page. This information will then be viewable to the website owner when accessing the session replay through the Session Replay Provider.

33. Session Replay Code does not necessarily anonymize user sessions, either.

34. First, if a user’s entry of personally identifying information is captured in an event response, that data will become known and visible to both the Session Replay Provider and the website owner.

35. Second, if a website displays user account information to a logged-in user, that content may be captured by Session Replay Code.

36. Third, some Session Replay Providers explicitly offer website owners cookie functionality that permits linking a session to an identified user, who may be personally identified if the website owner has associated the user with an email address or username.¹⁹

37. Session Replay Providers often create “fingerprints” that are unique to a particular user’s combination of computer and browser settings, screen configuration, and other detectable information. The resulting fingerprint, which is often unique to a user and rarely changes, are collected across all sites that the Session Replay Provider monitors.

¹⁹ *Id.*; see also *FS.identify – Identifying users*, FullStory, <https://help.fullstory.com/hc/en-us/articles/360020828113>, (last visited Sep. 8, 2022).

38. When a user eventually identifies themselves to one of these websites (such as by filling in a form), the provider can then associate the fingerprint with the user identity and can then back-reference all of that user’s other web browsing across other websites previously visited, including on websites where the user had intended to remain anonymous—even if the user explicitly indicated that they would like to remain anonymous by enabling private browsing.

39. In addition to the privacy invasions caused by the diversion of user communications with websites to third-party Session Replay Providers, Session Replay Code also exposes website visitors to identity theft, online scams, and other privacy threats.²⁰ Indeed, “[t]he more copies of sensitive information that exist, the broader the attack surface, and when data is being collected [. . .] it may not be stored properly or have standard protections” increasing “the overall risk that data will someday publicly leak or be breached.”²¹

40. Recognizing the privacy concerns posed by Session Replay Code, in 2019 Apple required app developers to remove or properly disclose the use of analytics code that allow app developers to record how a user interacts with their iPhone apps or face immediate removal from the app store.²² In announcing this decision, Apple stated: “Protecting user privacy is paramount in the Apple ecosystem. Our App Store Review Guidelines require that apps request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity.”²³

²⁰ Juha Sarrinen, *Session Replay is a Major Threat to Privacy on the Web*, itnews (Nov. 16, 2017), <https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720>.

²¹ Lily Hay Newman, *Covert ‘Replay Sessions’ Have Been harvesting Passwords by Mistake*, WIRED (Feb. 26, 2018), <https://www.wired.com/story/covert-replay-sessions-harvesting-passwords/>.

²² Zack Whittaker, *Apple Tells App Developers to Disclose or Remove Screen Recording Code*, TechCrunch (Feb. 7, 2019), <https://techcrunch.com/2019/02/07/apple-glassbox-apps/>.

²³ *Id.*

D. Defendants Secretly Wiretap Zillow’s Website Visitors’ Electronic Communications.

41. Zillow operates the Zillow website. Zillow is the “leading online residential real estate” marketplace in the United States for consumers, connecting them to the information and real estate professionals they need to buy, sell, or rent a home.²⁴

42. Zillow has become “synonymous with residential real estate.”²⁵ Zillow’s website is the most popular real estate website in the United States, with over thirty-six million unique monthly visitors²⁶ and more than 135 million properties are listed on its website.²⁷ According to a 2021 Google Trends report, “[t]oday more people search ‘Zillow’ than ‘real estate.’”²⁸

43. However, unbeknownst to the millions of individuals perusing Zillow’s real estate listings, Zillow intentionally procures and embeds various Session Replay Codes from Microsoft and other Session Replay Providers on its website to track and analyze website user interactions with Zillow’s website.

44. Zillow has procured Microsoft to employ its Session Replay Provider on Zillow’s website.

²⁴ Zillow Group, Inc., *Form 10-K* (Dec. 31, 2021), <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001617640/87bbbf30-39cb-4eb7-acdc-1b51265b9687.pdf> (“Zillow 10-K”).

²⁵ *Id.*

²⁶ *Most Popular Real Estate Websites in the United States as of October 2021, Based on Unique Monthly Visits*, Statista, <https://www.statista.com/statistics/381468/most-popular-real-estate-websites-by-monthly-visits-usa/>, (last visited Sep. 8, 2022).

²⁷ Zillow 10-K, *supra*, note 1.

²⁸ *Id.*

1 45. Microsoft is the owner and operator of a Session Replay Code called Clarity,
2 which provides basic information about website user sessions, interactions, and engagement,
3 and breaks down users by device type, county, and other dimensions.²⁹

4 46. Clarity captures a user's interactions with a website, logging every website
5 user's mouse movements and clicks, scrolling window resizing, user inputs, and more.³⁰
6 Indeed, Clarity organizes the information it captures into over 30 different categories including:
7 the date a user visited the website, the device the user accessed the website on, the type of
8 browser the user accessed the website on, the operating system of the device used to access the
9 website, the country where the user accessed the website from, a user's mouse movements, a
10 user's screen swipes, text inputted by the user on the website, and how far down a webpage a
11 user scrolls.³¹ Clarity even provides a specific user ID to each website visitor so their website
12 use and interactions can be monitored over time.³²

13 47. The information collected and recorded by Clarity can then be used to play back
14 a user's journey through a website, showing how they interacted with site navigation, calls to
15 action, search features, and other on-page elements.³³ Put differently, the information Clarity
16 captures can be translated into a simulation video of how a user interacts with a website.

17 48. Clarity also uses the information captured to create detailed heatmaps of a
18 website that provide information about which elements of a website have high user
19

20 _____
21 ²⁹ Jono Alderson, *An Introduction to Microsoft Clarity*, Yoast, <https://yoast.com/introduction-microsoft-clarity/#h-what-is-microsoft-clarity>, (last visited Sep. 8, 2022).

22 ³⁰ *Clarity Data Collection*, Microsoft, <https://docs.microsoft.com/en-us/clarity/clarity-data>, (last visited Aug. 24, 2022).

23 ³¹ *Filters Overview*, Microsoft (Jul. 26, 2022), <https://docs.microsoft.com/en-us/clarity/clarity-filters>.

³² *Id.*

³³ Roger Montti, *Microsoft Clarity Analytics: Everything You Need to Know*, SEJ (Jan. 19, 2022), <https://www.searchenginejournal.com/microsoft-clarity-analytics-overview/419311/#close>.

1 engagement, how far website users scrolled on the website, and the total clicks within a given
2 area on the website.³⁴

3 49. As such, Clarity collects highly personal information and substantive
4 communications that can be tied to directly to a website user's identity as it monitors, records,
5 and collects a website user's every move.

6 50. Clarity offers websites three standard approaches when it comes to masking
7 sensitive information collected from a user's interactions with a website: strict (all text entered
8 by a user is purportedly masked), balanced (sensitive text entered into certain specifically pre-
9 coded fields, such as passwords, and credit card information, is masked), and relaxed (no text
10 entered by a user is masked).³⁵ When Clarity is set to "relaxed," whatever information a user
11 enters into the field on a website can be previewed in session recordings.³⁶ Additionally,
12 Clarity enables websites to select specific elements and content to mask or unmask,
13 customizing the standard masking approaches.³⁷

14 51. However, even when a website operator selects the "strict" and "balanced"
15 settings, Clarity is nevertheless capable of collecting text entered by users, including text
16 containing sensitive information.

17 52. In order for Clarity to capture website visitors' interactions with a website,
18 Clarity's JavaScript must be installed on the website, either directly hard-coded on the website
19 or on a third-party platform, such as Google Tag Manager.³⁸ Clarity is embedded in a website
20

21 ³⁴ Haley Walden, *What is Microsoft Clarity? (& How Can it Improve SEO?)*, Elegant Themes (Jun. 12,
22 2022), <https://www.elegantthemes.com/blog/wordpress/microsoft-clarity-improve-seo>.

22 ³⁵ *Microsoft Clarity, An Essential Part of Customer Experience Optimization*, TechAir (Aug. 17, 2022),
23 <https://privacy.microsoft.com/en-US/privacystatement>.

³⁶ *Id.*

³⁷ *Masking Content*, Microsoft (Jul. 18, 2022), <https://docs.microsoft.com/en-us/clarity/clarity-masking>.

³⁸ *Set Up Clarity*, Microsoft (Jul. 18, 2022), <https://docs.microsoft.com/en-us/clarity/clarity-setup>.

1 by adding its JavaScript code into the HyperText Markup Language (HTML) underlying the
 2 website. As with all HTML code, Clarity is not visible to a user who is navigating a webpage
 3 through a standard browser's default view, because by design a browser will interpret HTML,
 4 without showing it, in order to render a more user-friendly display that is the designer's
 5 intended presentation of the website to a visitor.

6 53. Clarity can be revealed to technical users who understand web technologies and
 7 can enable alternative display modes that will show underlying HTML, such as “developer
 8 tools,” but even then, the users would first need to know what they are looking for to find the
 9 script. Developer tools are intended for website programmers, and are generally not meaningful
 10 or comprehensible by those without a background in computer science.

11 54. Once Clarity's JavaScript is installed on a website, Clarity begins collecting
 12 website user's interactions within two hours of installation.³⁹ Once deployed, Clarity the
 13 wiretapping commences immediately on the visitor's web browser when the visitor loads a
 14 website in their browser.

15 55. Data collected by Clarity is then stored in the Microsoft Aure cloud service and
 16 Microsoft has access to that information.⁴⁰

17 56. Zillow's procurement and use of Microsoft Clarity's Session Replay Code, and
 18 procurement and use of other Session Replay Codes through various Session Replay Providers,
 19 constitutes wiretapping in violation Washington statutory and common law.

20 **E. Plaintiffs' and Class Members' Experience.**

21
 22
 23 ³⁹ *Frequently Asked Questions*, Microsoft, <https://docs.microsoft.com/en-us/clarity/faq>, (last visited Aug. 24, 2022).

⁴⁰ *Id.*

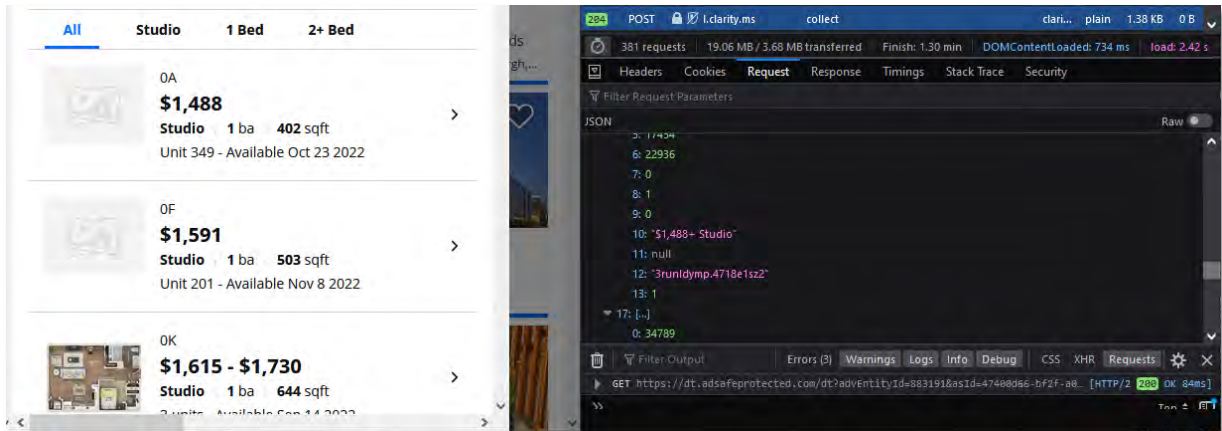
57. Plaintiff Perkins has visited Zillow's website on her computer during the period from April through June 2021. Plaintiff Perkins visited Zillow's website for the purposes of searching for and obtaining a rental apartment. During her visits made during the period April through June 2021, Plaintiff Perkins substantively engaged with Zillow's website and entered certain personal and financial information, such as her name, address, date of birth, phone number, social security number, and credit information into text fields..

58. Plaintiff Hasson routinely visits Zillow's website to search for properties using his computer, and he has done so numerous times throughout 2022. During his visits, including visits made during 2022, Plaintiff Hasson has substantively engaged with Zillow's website and has entered personal and financial information, such as name, address, date of birth, phone number, credit and financial information into text fields.

59. While visiting Zillow's website, Plaintiffs fell victim to Defendants' unlawful monitoring, recording, and collection of Plaintiffs' Website Communications with Zillow's website.

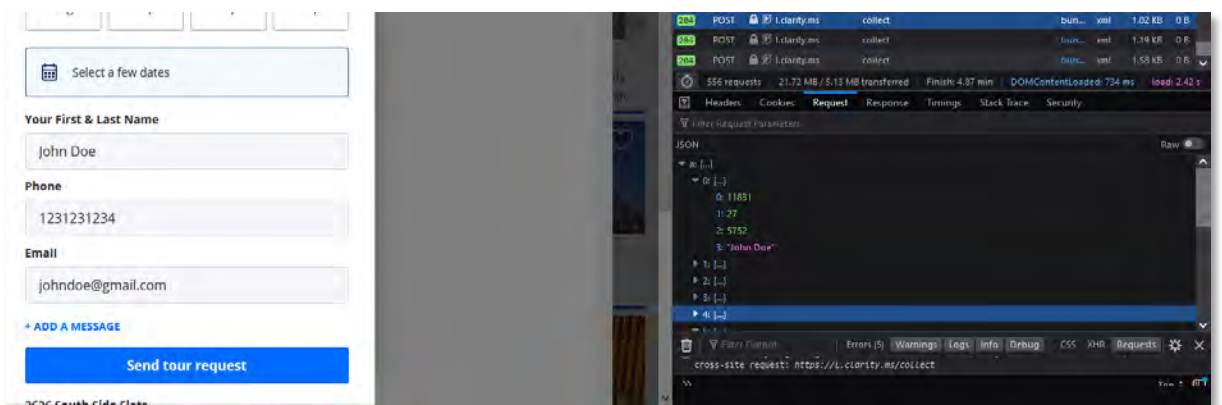
60. Unbeknownst to Plaintiffs, and without Plaintiffs' consent, Zillow procures and embeds Microsoft's Session Replay Code on its website. Plaintiffs' Website Communications were captured by Microsoft's Session Replay Code and sent to various Session Replay Providers.

61. For example, when visiting Zillow's website, if a website user views a certain piece of property for rent or sale, that information is captured by the Session Replay Codes embedded on the website:



Depicting information sent to one of the Service Replay Providers—Microsoft—through a Service Replay Code—Clarity—after viewing a Studio apartment priced at \$1,488 while visiting www.zillow.com.

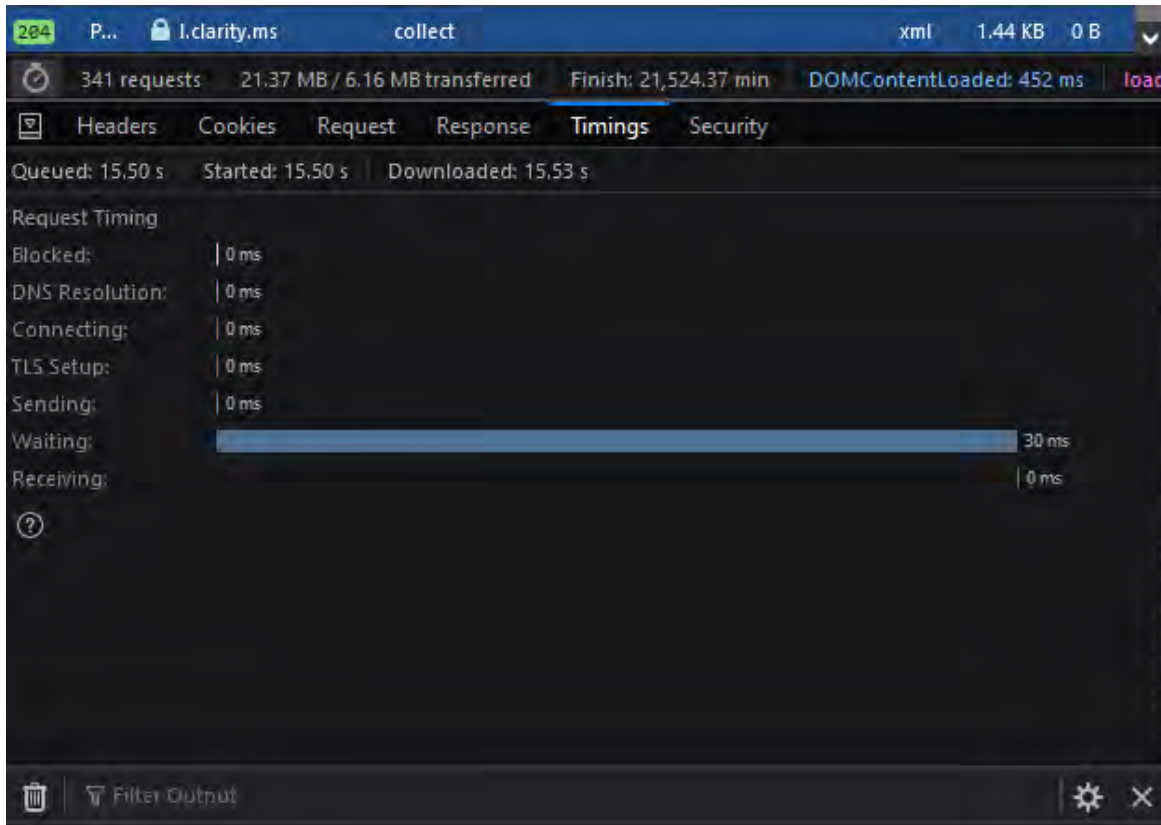
62. Similarly, when visiting Zillow’s website, if a user enters personal information in a text box to schedule a tour, that information is captured by the Session Replay Codes embedded on the website:



Depicting information sent to one of the Service Replay Providers—Microsoft—through a Service Replay Code—Clarity—after entering a name (purple text) to a text box to schedule a tour of a property.

63. The wiretapping by the Session Replay Codes are ongoing during the visit, and the Session Replay Code intercepts the contents of these communications between Plaintiffs and Zillow with instantaneous transmissions to Microsoft’s Session Replay software and other

Session Replay Providers, as illustrated below, in which only 30 milliseconds were required to send a packet of even response data, which would indicate whatever the website user had just done:



64. The Session Replay Codes operate in the same manner for all putative Class members.

65. Like Plaintiffs, each Class member visited Zillow's website with Microsoft's and other Session Replay Providers' Code embedded in it. Those Session Replay Codes intercepted the Class members' Website Communications with Zillow's website by sending hyper-frequent logs of those communications to Session Replay Providers.

66. Even if Zillow masks certain elements when it configures the settings of the Session Replay Code embedded on its website, any operational iteration of the Session Replay

Code will, by its very nature and purpose, intercept the contents of communications between the website's visitors and the website owner.

67. For example, even with heightened masking enabled, Defendants—through the use of Session Replay Providers' Code—are still able to learn through the intercepted data exactly which pages a user navigates to, how the user moves through the page (such as which areas the user zooms in on or interacted with), and additional substantive information.

68. As a specific example, if a user types a particular address or zip code into Zillow's main search bar and initiates a search, even if the text entered into the search bar is masked, Session Replay Providers will still learn what is entered into the bar as soon as the search result page loads. This is so because the responsive search results will be displayed on the subsequent page, and the responsive content generated by Zillow will repeat the searched information back on the generated page. That information will not be masked even if user-inputted text is fully masked in a text field.

CLASS ACTION ALLEGATIONS

69. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Class:

All natural persons in the United States and its territories whose Website Communications were captured through the use of Session Replay Code embedded in Zillow's website

70. Excluded from the Class are Defendants, their parents, subsidiaries, affiliates, officers, and directors, all persons who make a timely election to be excluded from the Class, the judge to whom this case is assigned and any of the judge's immediate family members, and the attorneys who enter their appearance in this action.

1 71. **Numerosity:** The members of the Class are so numerous that individual joinder
 2 of all Class members is impracticable. The precise number of Class members and their
 3 identities may be obtained from the books and records of Defendants or other Session Replay
 4 Providers.

5 72. **Commonality:** This action involves questions of law and fact that are common
 6 to the Class members. Such common questions include, but are not limited to: (a) whether
 7 Zillow procured Microsoft and other Session Replay Providers to intercept Zillow's website
 8 visitors' Website Communications; (b) whether Defendants intentionally disclosed the
 9 intercepted Website Communications of Zillow's website users; (c) whether Defendants
 10 acquire the contents of website users' Website Communications without their consent; (d)
 11 whether Defendants' conduct violates Washington Wiretapping Statute, Wash. Rev. Code
 12 §9.73.030, *et seq.*; (e) whether Plaintiffs and the Class members are entitled to equitable relief;
 13 and (f) whether Plaintiffs and the Class members are entitled to actual, statutory, punitive, or
 14 other forms of damages, and other monetary relief.

15 73. **Typicality:** Plaintiffs' claims are typical of the other Class members' claims
 16 because, among other things, all Class members were comparably injured through the uniform
 17 prohibited conduct described above. For instance, Plaintiffs and each member of the Class had
 18 their communications intercepted in violation of the law and their right to privacy. This
 19 uniform injury and the legal theories that underpin recovery make the claims of Plaintiffs and
 20 the members of the Class typical of one another.

21 74. **Adequacy of Representation:** Plaintiffs have and will continue to fairly and
 22 adequately represent and protect the interests of the Class. Plaintiffs have retained counsel
 23 competent and experienced in complex litigation and class actions, including litigations to

1 remedy privacy violations. Plaintiffs have no interest that is antagonistic to the interests of the
 2 Class, and Defendants have no defenses unique to Plaintiffs. Plaintiffs and their counsel are
 3 committed to vigorously prosecuting this action on behalf of the members of the Class, and
 4 they have the resources to do so. Neither Plaintiffs nor their counsel have any interest adverse
 5 to the interests of the other members of the Class.

6 75. **Superiority:** This class action is appropriate for certification because class
 7 proceedings are superior to other available methods for the fair and efficient adjudication of
 8 this controversy and joinder of all members of the Class is impracticable. This proposed class
 9 action presents fewer management difficulties than individual litigation, and provides the
 10 benefits of single adjudication, economies of scale, and comprehensive supervision by a single
 11 court. Class treatment will create economies of time, effort, and expense and promote uniform
 12 decision-making.

13 76. **Predominance:** Common questions of law and fact predominate over any
 14 questions affecting only individual Class members. Similar or identical violations, business
 15 practices, and injuries are involved. Individual questions, if any, pale by comparison, in both
 16 quality and quantity, to the numerous common questions that dominate this action. For
 17 example, Defendants' liability and the fact of damages is common to Plaintiffs and each
 18 member of the Class. If Defendants intercepted Plaintiffs' and Class members' Website
 19 Communications, then Plaintiffs and each Class member suffered damages by that conduct.

20 77. **Ascertainability:** Members of the Class are ascertainable. Class membership is
 21 defined using objective criteria and Class members may be readily identified through
 22 Defendants' books and records or the other Session Replay Providers' books and records.
 23

CHOICE OF LAW

78. Defendants' actions discussed herein were orchestrated and implemented by Zillow at its corporate headquarters in Washington, and the conduct Plaintiffs complains of occurred in, and radiated from, Washington.

79. The key wrongdoing at issue in this litigation (Zillow's procurement of Microsoft and other Session Replay Providers to intercept Zillow's website visitors' Website Communications; Zillow's intentional disclosure of the intercepted Website Communications of its website users; Zillow's acquisition of the contents of website users' Website Communications without their consent; and Zillow's and Microsoft's violation of the Washington Wiretap Statute) emanated from Defendants' respective headquarters located in Washington.

80. Moreover, Zillow's Terms of Use specifically state that the "Terms of Use are governed by the laws of the State of Washington, without giving effect to its conflict of laws' provisions." <https://www.zillowgroup.com/terms-of-use/>. Moreover, Zillow states that users of its website "agree to submit to the personal and exclusive jurisdiction and venue in the state and federal courts sitting in King County, Washington for any and all disputes, claims and actions arising from or in connection with the Services or otherwise under these Terms of Use." <https://www.zillowgroup.com/terms-of-use/>.

81. Washington, which seeks to protect the rights and interests of Washington and other U.S. consumers against a company doing business in Washington, has a greater interest in the claims of Plaintiffs and the Class than any other state and is most intimately concerned with the outcome of this litigation.

82. Application of Washington law to a nationwide Class with respect to Plaintiffs' and the Class's claims is neither arbitrary nor fundamentally unfair because Washington has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiffs and the nationwide Class.

COUNT I
Violation of the Washington Wiretapping Statute
Wash. Rev. Code §9.73.030, et. seq.

83. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

84. Plaintiffs bring this claim individually and on behalf of the Class against Defendants.

85. The Washington Wiretapping Statute (the "Act") prohibits the interception or recording any private communication transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state by any device electronic or otherwise designed to record and/or transmit said communication regardless how such device is powered or actuated, without first obtaining the consent of all the participants in the communication. Wash. Rev. Code §9.73.030(1)(a).

86. The Act further states that "[a]ny person who, directly or by means of a detective agency or any other agent, violates the provisions of this chapter shall be subject to legal action for damages, to be brought by any other person claiming that a violation of this statute has injured his or her business, his or her person, or his or her reputation. A person so injured shall be entitled to actual damages, including mental pain and suffering endured by him or her on account of violation of the provisions of this chapter, or liquidated damages computed at the rate of one hundred dollars a day for each day of violation, not to exceed one thousand

dollars, and a reasonable attorney's fee and other costs of litigation." Wash. Rev. Code §9.73.060.

87. Zillow and Microsoft are persons for purposes of the Act because they are corporations.

88. Session Replay Code like that licensed by Microsoft and procured by Zillow is a "device" that is "designed to record and/or transmit" communications within the meaning of the Act.

89. Plaintiffs' and Class members' intercepted Website Communications constitute "private communications" within the meaning of the Act.

90. Defendants intentionally procure and embed Microsoft's Session Replay Code and other Session Replay Providers Code on Zillow's website to spy on, automatically and secretly, and to intercept Zillow's website visitors' electronic interactions communications with Zillow in real time.

91. Plaintiffs' and Class members' electronic communications are intercepted contemporaneously with their transmission.

92. Plaintiffs and Class members did not consent to having their Website Communications wiretapped.

93. Pursuant to Wash. Rev. Code §9.73.060, Plaintiffs and the Class members seek (1) actual damages, not less than liquidated damages computed at the rate of one hundred dollars a day for each day of violation, not to exceed one thousand dollars, and (2) reasonable attorneys' fees and other costs of litigation incurred.

94. Defendants' conduct is ongoing, and they continue to unlawfully intercept the communications of Plaintiffs and Class members any time they visit Zillow's website with

1 Microsoft's Session Replay Code enabled without their consent. Plaintiffs and Class members
2 are entitled to declaratory and injunctive relief to prevent future interceptions of their
3 communications and to require Zillow to obtain consent prior to utilizing Microsoft's Session
4 Replay Code and other Session Replay Providers Code to intercept website visitors' electronic
5 communications on Zillow's website.

6
7 **COUNT II**
Invasion of Privacy – Intrusion Upon Seclusion

8 95. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

9 96. Washington common law recognizes the tort of invasion of privacy. The right to
10 privacy is also established in the Constitution of the State of Washington which explicitly
11 recognizes an individual's right to privacy under Article 1 §7: "No person shall be disturbed in
12 his private affairs, or his home invaded, without authority of law."

13 97. Plaintiffs bring this claim individually and on behalf of the Class.

14 98. Plaintiffs and Class members have an objective, reasonable expectation of
15 privacy in their Website Communications.

16 99. Plaintiffs and Class members did not consent to, authorize, or know about
17 Defendants' intrusion at the time it occurred. Plaintiffs and Class members never agreed that
18 Defendants could collect or disclose their Website Communications.

19 100. Plaintiffs and Class members had a legitimate and reasonable expectation of
20 privacy in precluding the dissemination and/or misuse of their information and communications
21 and in conducting their personal activities without intrusion or interference, including the right
22 to not have their personal information intercepted and utilized for business gain.

23 101. Defendants intentionally intrude on Plaintiffs' and Class members' private life,
seclusion, or solitude, without consent.

102. Defendants' conduct is highly offensive and objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

103. Defendants' conduct, by unlawfully intercepting the communications of Plaintiffs and Class members any time they visit Zillow's website with Microsoft's Session Replay Code enabled without their consent, was a proximate cause of damage to Plaintiffs and Class members.

104. Plaintiffs and Class members were harmed by Defendants' wrongful conduct as Defendants' conduct has caused Plaintiffs and the Class mental anguish and suffering arising from their loss of privacy and confidentiality of their electronic communications.

105. Defendants' conduct has needlessly harmed Plaintiffs and the Class by capturing intimately personal facts and data in the form of their Website Communications. This disclosure and loss of privacy and confidentiality has caused Plaintiffs and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

106. Additionally, given the monetary value of individual personal information, Defendants deprived Plaintiffs and Class members of the economic value of their interactions with Defendant's website, without providing proper consideration for Plaintiffs' and Class members' property.

107. Further, Defendants have improperly profited from their invasion of Plaintiffs and Class members' privacy in their use of this data for their economic gain.

108. As a direct and proximate result of Defendants conduct, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

109. Defendants' conduct is ongoing, and they continue to unlawfully intercept the communications of Plaintiffs and Class members any time they visit Zillow's website with Microsoft's Session Replay Code and other Session Replay Providers Code enabled without their consent. Plaintiffs and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

REQUEST FOR RELIEF

Plaintiffs, individually and on behalf of themselves and the other members of the proposed Class, respectfully request that the Court enter judgment in Plaintiffs' and the Class's favor and against Defendants as follows:

- A. Certifying the Class and appointing Plaintiffs as the Class representatives;
- B. Appointing Plaintiffs' counsel as class counsel;
- C. Declaring that Defendants' past conduct was unlawful, as alleged herein;
- D. Declaring Defendants' ongoing conduct is unlawful, as alleged herein;
- E. Enjoining Defendants from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;
- F. Awarding Plaintiffs and the Class members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;
- G. Awarding Plaintiffs and the Class members pre-judgment and post-judgment interest;
- H. Awarding Plaintiffs and the Class members reasonable attorneys' fees, costs, and expenses; and
- I. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the Class, demand a trial by jury of any and all issues in this action so triable of right.

DATED this 12th day of September, 2022.

TOUSLEY BRAIN STEPHENS PLLC

By: s/ Kim D. Stephens, P.S.
Kim D. Stephens, P.S., WSBA #11984
kstephens@tousley.com
s/ Jason T. Dennett
Jason T. Dennett, WSBA #30686
jdennett@tousley.com
s/ Kaleigh N. Boyd
Kaleigh N. Boyd, WSBA #52684
kboyd@tousley.com
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
Telephone: 206.682.5600
Fax: 206.682.2992

Joseph P. Guglielmo, (*pro hac vice* forthcoming)
Carey Alexander (*pro hac vice* forthcoming)
Ethan Binder (*pro hac vice* forthcoming)
**SCOTT+SCOTT ATTORNEYS
AT LAW LLP**
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: (212) 223-6444
Facsimile: (212) 223-6334
jguglielmo@scott-scott.com
calexander@scott-scott.com
ebinder@scott-scott.com

1 E. Kirk Wood (*pro hac vice* forthcoming)
2 Sharika Robinson (*pro hac vice* forthcoming)
3 Marcela Jenkins (*pro hac vice* forthcoming)
4 **WOOD LAW FIRM, LLC**
5 P. O. Box 382434
6 Birmingham, AL 35238-2434
7 Telephone: (205) 908-4906
8 kirk@woodlawfirmllc.com

9 Gary F. Lynch (*pro hac vice* forthcoming)
10 Kelly K. Iverson (*pro hac vice* forthcoming)
11 Jamisen A. Etzel (*pro hac vice* forthcoming)
12 Elizabeth Pollock-Avery (*pro hac vice* forthcoming)
13 Nicholas A. Colella (*pro hac vice* forthcoming)
14 Patrick D. Donathen (*pro hac vice* forthcoming)
15 **LYNCH CARPENTER, LLP**
16 1133 Penn Avenue, 5th Floor
17 Pittsburgh, Pennsylvania 15222
18 Telephone: 412-322-9243
19 Facsimile: 412-231-0246
20 gary@lcllp.com
21 kelly@lcllp.com
22 jamisen@lcllp.com
23 elizabeth@lcllp.com
nickc@lcllp.com
patrick@lcllp.com

Attorneys for Plaintiffs and the Putative Class

[Query](#) [Reports](#) [Utilities](#) [Help](#) [Log Out](#)

JURYDEMAND

U.S. District Court
United States District Court for the Western District of Washington (Seattle)
CIVIL DOCKET FOR CASE #: 2:22-cv-01282-SKV

Perkins et al v. Zillow Group Inc et al
Assigned to: Hon. S. Kate Vaughan
Cause: 28:1332 Diversity

Date Filed: 09/12/2022
Jury Demand: Plaintiff
Nature of Suit: 380 Personal Property: Other
Jurisdiction: Diversity

Plaintiff

Natalie Perkins

represented by **Carey Alexander**
SCOTT + SCOTT LLP (NY)
THE HELMSLEY BUILDING
230 PARK AVE
STE 17TH FLOOR
NEW YORK, NY 10169
212-223-6444
Email: calexander@scott-scott.com
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Ethan Binder
SCOTT + SCOTT LLP (NY)
THE HELMSLEY BUILDING
230 PARK AVE
STE 17TH FLOOR
NEW YORK, NY 10169
212-223-6444
Fax: 212-233-6334
Email: ebinder@scott-scott.com
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jason T Dennett
TOUSLEY BRAIN STEPHENS
1200 FIFTH AVE STE 1700
SEATTLE, WA 98101
206-682-5600
Fax: 206-682-2992
Email: jdennett@tousley.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph P Guglielmo
SCOTT + SCOTT LLP (NY)

THE HELMSLEY BUILDING
230 PARK AVE
STE 17TH FLOOR
NEW YORK, NY 10169
212-223-6444
Email: jguglielmo@scott-scott.com
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Kaleigh Boyd
TOUSLEY BRAIN STEPHENS
1200 FIFTH AVE STE 1700
SEATTLE, WA 98101
206-682-5600
Fax: 206-682-2992
Email: kboyd@tousley.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kim D Stephens
TOUSLEY BRAIN STEPHENS
1200 FIFTH AVE STE 1700
SEATTLE, WA 98101
206-682-5600
Email: kstephens@tousley.com
ATTORNEY TO BE NOTICED

Plaintiff

Kenneth Hasson

represented by **Carey Alexander**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Ethan Binder
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jason T Dennett
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph P Guglielmo
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Kaleigh Boyd
(See above for address)

LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kim D Stephens
(See above for address)
ATTORNEY TO BE NOTICED

V.

Defendant

Zillow Group Inc

Defendant

Microsoft Corporation

represented by **Anna Mouw Thompson**
PERKINS COIE (SEA)
1201 3RD AVE STE 4900
SEATTLE, WA 98101-3099
206-359-8000
Email: AnnaThompson@perkinscoie.com
ATTORNEY TO BE NOTICED

Nicola Menaldo
PERKINS COIE (SEA)
1201 3RD AVE STE 4900
SEATTLE, WA 98101-3099
206-359-3787
Email: NMenaldo@perkinscoie.com
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
09/12/2022	<u>1</u>	COMPLAINT against defendant(s) Microsoft Corporation, Zillow Group Inc with JURY DEMAND (Receipt # AWAADC-7697512) Attorney Kim D Stephens added to party Kenneth Hasson(pty:pla), Attorney Kim D Stephens added to party Natalie Perkins(pty:pla), filed by Natalie Perkins, Kenneth Hasson. (Attachments: # <u>1</u> Civil Cover Sheet, # <u>2</u> Summons, # <u>3</u> Summons)(Stephens, Kim) (Entered: 09/12/2022)
09/15/2022		Hon. S. Kate Vaughan added. (RE) (Entered: 09/15/2022)
09/15/2022	<u>2</u>	Summons(es) Electronically Issued as to defendant(s) Microsoft Corporation, Zillow Group Inc. (Attachments: # <u>1</u> Summons) (RE) (Entered: 09/15/2022)
09/20/2022	<u>3</u>	APPLICATION OF ATTORNEY Ethan Binder FOR LEAVE TO APPEAR PRO HAC VICE for Plaintiffs Kenneth Hasson, Natalie Perkins (Fee Paid) Receipt No. AWAADC-7708578 (Stephens, Kim) (Entered: 09/20/2022)
09/20/2022	<u>4</u>	APPLICATION OF ATTORNEY Carey Alexander FOR LEAVE TO APPEAR PRO HAC VICE for Plaintiffs Kenneth Hasson, Natalie Perkins (Fee Paid) Receipt No. AWAADC-7708594 (Stephens, Kim) (Entered: 09/20/2022)
09/20/2022	<u>5</u>	APPLICATION OF ATTORNEY Joseph P. Guglielmo FOR LEAVE TO APPEAR PRO HAC VICE for Plaintiffs Kenneth Hasson, Natalie Perkins (Fee Paid) Receipt No. AWAADC-7708605 (Stephens, Kim) (Entered: 09/20/2022)
09/20/2022	6	ORDER re <u>4</u> Application for Leave to Appear Pro Hac Vice. The Court ADMITS

		Attorney Carey Alexander for Plaintiffs Kenneth Hasson and Natalie Perkins by Clerk Ravi Subramanian. No document associated with this docket entry, text only. <i>NOTE TO COUNSEL: Local counsel agrees to sign all filings and to be prepared to handle the matter, including the trial thereof, in the event the applicant is unable to be present on any date scheduled by the court, pursuant to LCR 83.1(d). (JWC) (Entered: 09/20/2022)</i>
09/20/2022	7	ORDER re 5 Application for Leave to Appear Pro Hac Vice. The Court ADMITS Attorney Joseph P Guglielmo for Plaintiffs Kenneth Hasson and Natalie Perkins by Clerk Ravi Subramanian. No document associated with this docket entry, text only. <i>NOTE TO COUNSEL: Local counsel agrees to sign all filings and to be prepared to handle the matter, including the trial thereof, in the event the applicant is unable to be present on any date scheduled by the court, pursuant to LCR 83.1(d). (JWC) (Entered: 09/20/2022)</i>
09/20/2022	8	ORDER re 3 Application for Leave to Appear Pro Hac Vice. The Court ADMITS Attorney Ethan Binder for Plaintiffs Kenneth Hasson and Natalie Perkins by Clerk Ravi Subramanian. No document associated with this docket entry, text only. <i>NOTE TO COUNSEL: Local counsel agrees to sign all filings and to be prepared to handle the matter, including the trial thereof, in the event the applicant is unable to be present on any date scheduled by the court, pursuant to LCR 83.1(d). (JWC) (Entered: 09/20/2022)</i>
10/04/2022	9	AFFIDAVIT of Service of Summons and Complaint on Microsoft Corporation on 9/28/2022, filed by Plaintiffs Kenneth Hasson, Natalie Perkins. (Guglielmo, Joseph) (Entered: 10/04/2022)
10/04/2022	10	WAIVER OF SERVICE of Summons upon defendant Zillow Group Inc mailed on 9/29/2022 (Guglielmo, Joseph) (Entered: 10/04/2022)
10/18/2022	11	NOTICE of Appearance by attorney Nicola Menaldo on behalf of Defendant Microsoft Corporation. (Menaldo, Nicola) (Entered: 10/18/2022)
10/18/2022	12	NOTICE of Appearance by attorney Anna Mouw Thompson on behalf of Defendant Microsoft Corporation. (Thompson, Anna) (Entered: 10/18/2022)
10/18/2022	13	APPLICATION OF ATTORNEY James G. Snell FOR LEAVE TO APPEAR PRO HAC VICE for Defendant Microsoft Corporation (Fee Paid) Receipt No. AWAWDC-7744302 (Menaldo, Nicola) (Entered: 10/18/2022)
10/18/2022	14	Stipulated MOTION TO EXTEND DEFENDANT MICROSOFT CORPORATIONS RESPONSIVE PLEADING DEADLINE, filed by Defendant Microsoft Corporation. Noting Date 10/18/2022, (Menaldo, Nicola) (Entered: 10/18/2022)
10/18/2022	15	CORPORATE DISCLOSURE STATEMENT indicating no Corporate Parents and/or Affiliates. Filed pursuant to Fed.R.Civ.P 7.1. Filed by Microsoft Corporation (Menaldo, Nicola) (Entered: 10/18/2022)

PACER Service Center

Transaction Receipt

10/19/2022 08:42:22

PACER

samanthasouthall

Client Code:

0106198-000001-SS

Login:			
Description:	Docket Report	Search Criteria:	2:22-cv-01282-SKV
Billable Pages:	4	Cost:	0.40

**UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

JILL STRELZIN, individually and on)	
behalf of all others similarly situated,)	
)	
Plaintiff,)	Case No. 1:22-cv-05644
)	
vs.)	(Circuit Court of Cook County, Illinois,
)	County Department – Chancery Division, Case
ZILLOW GROUP, INC.,)	No. 2022CH09132)
)	
Defendant.)	
)	

NOTICE OF REMOVAL

PLEASE TAKE NOTICE that Defendant Zillow Group, Inc. (“Zillow”), by and through its undersigned counsel, hereby files this Notice of Removal pursuant to 28 U.S.C. §§ 1441 and 1446, removing this action from the Circuit Court of Cook County, Illinois County Department – Chancery Division, Case No. 2022CH09132, in which it is now pending, to the United States District Court for the Northern District of Illinois, on the grounds that there is jurisdiction in this Court pursuant to 28 U.S.C. § 1332(a). In support of this Notice of Removal, Zillow respectfully states the following:

1. On September 15, 2022, Jill Strelzin (“Plaintiff”) filed a Putative Class Action Complaint against Zillow in the Circuit Court of Cook County, Illinois County Department – Chancery Division, Case No. 2022CH09132 (the “State Court Action”). In compliance with 28 U.S.C. § 1446(a), a true and correct copy of the Complaint in the State Court Action is attached as Exhibit A.

2. On September 15, 2022, Zillow was served with original process.

3. Pursuant to 28 U.S.C. § 1446(d), written notice of the removal of this action shall be promptly served upon Plaintiff and Notice of Filing with the Clerk for the Circuit Court of Cook County. A true and correct copy of the proposed Notice of Filing of Notice of Removal is attached as Exhibit B.

JURISDICTION

4. This Court has original jurisdiction, and this action is properly removable, pursuant to the Class Action Fairness Act of 2005 (“CAFA”). *See* 28 U.S.C. §§ 1332, 1446, and 1453. The amount in controversy exceeds \$5 million. There are more than 100 putative class members. The members of the putative class are citizens of the State of Illinois. Defendant is a Washington citizen.

5. CAFA defines a class action as “any civil action filed under [R]ule 23 of the Federal Rules of Civil Procedure or similar State statute or rule of judicial procedure authorizing an action to be brought by one or more representative persons as a class action.” *See* 28 U.S.C. §§ 1332(d)(1)(B), 1453(a). The Complaint falls within this definition because Plaintiff brings this action pursuant to 735 ILCS 5/2-801, individually and on behalf of a putative class. (Compl. at ¶ 57).

6. While Plaintiff does not make any allegations about the size of her proposed class, two complaints filed in this Court, asserting substantially similar claims likewise on behalf of an Illinois class, assert that the putative classes in those cases contain more than 100 individuals. Attached hereto as Exhibit C is a true and correct copy of the complaint in *Ryan Margulis v. Zillow Group, Inc.*, Case 1:22-cv-04847 (N.D. Ill.) (*see* ¶ 7); attached hereto as Exhibit D is a true and correct copy of the complaint in *Mark Conlisk and Michael Dekhtyar v. Zillow Group, Inc.*, Case 1:22-cv-05082 (N.D. Ill.) (*see* ¶ 9). Moreover, as of August 4, 2022, Zillow has 234 million

average monthly unique users. Zillow Group, Inc., Current Report (Form 8-K - Ex-99.3) (Aug. 4, 2022). And, as of July 1, 2021, Illinois had a population of 12,671,469. *See* <https://www.census.gov/quickfacts/fact/table/IL> (last visited October 4, 2022). It is therefore plausible that a minimum of 100 individuals, from Zillow’s 234 million monthly unique users, were located in Illinois.

7. CAFA defines diversity citizenship as “any member of a class of Plaintiffs [who] is a citizen of a State different from any Defendant.” *See* 28 U.S.C. §§ 1332(d)(2)(A). This requirement is satisfied here. Plaintiff is a citizen of Illinois. *See* Compl. at ¶ 5. As further alleged in the Complaint, Zillow is both headquartered in and organized under the laws of Washington. *Id.* at ¶ 6. For diversity purposes, a corporation is deemed a citizen of the states in which it is incorporated and where it has its principal place of business, which is defined as its “nerve center.” *See* 28 U.S.C. § 1332(c)(1); *Hertz Corp. v. Friend*, 559 U.S. 77, 93 (2010) (“A corporation’s ‘nerve center,’ usually its main headquarters, is a single place.”). Therefore, Zillow is a citizen of Washington. Because Plaintiff is a citizen of Illinois and Zillow is a citizen of Washington, there is complete diversity of citizenship among the parties, and federal diversity exists under 28 U.S.C. § 1332(a). Moreover, there has been complete diversity of citizenship at all relevant times. *See Kanzelberger v. Kanzelberger*, 782 F.2d 774, 776 (7th Cir. 1986).

8. The claims of individual class members can be aggregated to determine if the amount in controversy exceeds the required “sum or value of \$5,000,000, exclusive of interest and costs.” 28 U.S.C. §§ 1332(d)(2), (d)(6). Here, the amount in controversy exceeds \$5 million.¹

¹ Zillow denies Plaintiff’s substantive allegations, the appropriateness of class treatment, that Plaintiff is entitled to any of the relief she seeks in her Complaint, and does not waive any defense with respect to any of Plaintiff’s claims. Nonetheless, the amount in controversy is properly determined by accepting Plaintiff’s allegations as true. *See Brill v. Countrywide Home Loans, Inc.*, 427 F.3d 446, 448 (7th Cir. 2005).

See 720 ILCS 5/14-16 (permitting recovery of actual damages and punitive damages); 815 ILCS 505/10a(c) (giving express authority to award “reasonable attorney’s fees and costs” to prevailing plaintiffs for violations of Illinois’ Consumer Fraud and Deceptive Business Practices Act); *Straits Fin. LLC v. Ten Sleep Cattle Co.*, 900 F.3d 359, 373 (7th Cir. 2018) (“allow[ing] fee awards for work on an ICFA claim and for work on non-Act claims when the Act claim is so inextricably intertwined with the non-Act claims that it cannot be distinguished.”) (citation omitted); Ex. C at ¶ 7; Ex. D at ¶ 9.

9. Plaintiff’s putative Class Action Complaint alleges three causes of action against Zillow: (i) a putative class claim for violation of Illinois’ Eavesdropping Act, 720 ILCS 5/14-1 *et seq.*; (ii) a putative class claim for violation of Illinois’ Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.*; and (iii) a putative class claim for the tort of common law invasion of privacy/intrusion upon seclusion. All three claims arise from Plaintiff’s and putative class members’ use of Zillow’s website.

10. Plaintiff seeks to recover actual damages, punitive damages, and attorneys’ fees. She also seeks an injunction, restitution, and disgorgement, as well as interest. Compl. at ¶¶ 83, 99 and Prayer for Relief, ¶¶ F-G.

11. “[A] defendant’s notice of removal need include only a plausible allegation that the amount in controversy exceeds the jurisdictional threshold.” *Dart Cherokee Basin Operating Co., LLC v. Owens*, 574 U.S. 81, 89 (2014). During the three months ended June 30, 2022, Zillow generated total gross profits of \$443 million. See Zillow Group, Inc., Quarterly Report (Form 10-Q) (Aug. 4, 2022). In light of Plaintiff’s request for “disgorgement of profits unlawfully obtained,” it is plausible that Plaintiff’s claims could surpass \$5 million.

12. The Action does not fall within any of exclusion to removal jurisdiction recognized by 28 U.S.C. § 1332(d), and the Plaintiffs have the burden of proving otherwise.

13. Zillow submits this Notice of Removal without waiving any defenses to the claims Plaintiff asserts, without conceding the Plaintiff has pleaded claims upon which relief can be granted, and without admitting that Plaintiff is entitled to any monetary or equitable relief whatsoever (or that the damages Plaintiff seeks may be properly sought).

CONCLUSION

WHEREFORE, Defendant Zillow Group, Inc, removes this civil action from the Circuit Court of Cook County to the United States District Court for the Northern District of Illinois.

Respectfully submitted,

Dated: October 14, 2022

BUCHANAN INGERSOLL & ROONEY PC

By: /s/ David T. Cellitti

David T. Cellitti (Bar No. 6272041)
401 E. Jackson Street, Suite 2400
Tampa, FL 33602
T: 813-222-8180
david.cellitti@bipc.com

Samantha L. Southall (*Pro Hac Vice* forthcoming)
50 S. 16th Street, Suite 3200
Philadelphia, PA 19102
T: 215-665-8700 | F: 215-665-8760
samantha.southall@bipc.com

Counsel for Defendant Zillow Group, Inc.

CERTIFICATE OF SERVICE

I, David T. Cellitti, hereby certify that I caused a copy of the foregoing Notice of Removal to be served by e-mail on counsel for Plaintiff on October 14, 2022:

Katrina Carroll, Esquire
Kyle Shamberg, Esquire
LYNCH CARPENTER LLP
111 W. Washington Street, Suite 1240
Chicago, IL 60602
T: 312-750-1265 | F: 773-598-5609
katrina@lcllp.com
kyle@lcllp.com

Gary Lynch, Esquire
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
T: 412-332-9243 | F: 412-231-0246
gary@lcllp.com

Counsel for Plaintiff and the Putative Class

/s/ David T. Cellitti

David T. Cellitti

Counsel for Defendant Zillow Group, Inc.

Dated: October 14, 2022

Exhibit A

Hearing Date: 1/13/2023 9:30 AM
Location: Court Room 2301
Judge: Quish, Clare J

**IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT – CHANCERY DIVISION**

FILED
9/15/2022 11:05 AM
IRIS Y. MARTINEZ
CIRCUIT CLERK
COOK COUNTY, IL
2022CH09132
Calendar, 14
19503961

JILL STRELZIN, individually and on behalf
of all others similarly situated,

Plaintiff,

Case No. _____

v.

2022CH09132

ZILLOW GROUP, INC.,

Defendant.

CLASS ACTION COMPLAINT

Plaintiff Jill Strelzin (“Plaintiff”), individually and on behalf of all others similarly situated, hereby files this class action complaint against Defendant Zillow Group, Inc. (“Defendant” or “Zillow”), and in support thereof alleges the following:

INTRODUCTION

1. This is a class action brought against Zillow for surreptitiously intercepting the private electronic communications of visitors to its website, www.zillow.com, without their consent. Zillow knowingly directs third-party vendors, such as Microsoft Corporation, to embed snippets of JavaScript computer code (“Session Replay Code”) on Zillow’s website, which then deploys on each website visitor’s internet browser for the purpose intercepting and recording the website visitor’s private electronic communications with the Zillow website, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time (“Website Communications”). These third-party vendors (collectively, “Session Replay Providers”) create and deploy the Session Replay Code at Zillow’s request.

2. After intercepting and recording the Website Communications, Zillow and the Session Replay Providers use those Website Communications to recreate website visitors' entire visit to www.zillow.com. The Session Replay Providers create a video replay of the user's behavior on the website and provide it to Zillow for analysis. Zillow's directive to the Session Replay Providers to secretly deploy the Session Replay Code results in the electronic equivalent of "looking over the shoulder" of each visitor to the Zillow website for the entire duration of their website interaction.

3. Zillow's conduct violates the Illinois Eavesdropping Act, 720 ILCS 5/14-1, *et seq.*, the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.*, and constitutes an invasion of the privacy rights of website visitors.

4. Plaintiff brings this action individually and on behalf of a class of all Illinois citizens whose Website Communications were intercepted at Zillow's direction and use of Session Replay Code embedded on the webpages of www.zillow.com and seeks all civil remedies provided under the causes of action, including but not limited to compensatory, statutory, and/or punitive damages, and attorneys' fees and costs.

PARTIES

5. Plaintiff is a citizen of the state of Illinois, and at all times relevant to this action, resided and was domiciled in Cook County, Illinois. Plaintiff is a citizen of Illinois.

6. Defendant Zillow Group, Inc. is corporation organized under the laws of Washington, and its principal place of business is located at 1301 Second Ave., Floor 31, Seattle Washington, 98101. Defendant is a citizen of Washington.

JURISDICTION AND VENUE

7. No federal question is presented by this complaint. Plaintiff brings this complaint solely under state law and not under federal law, and specifically not under the United States Constitution, nor any of its amendments, nor under 42 U.S.C. § 1981 or 1982, nor any other federal statute, law, rule, or regulation. Plaintiff believes and alleges that a cause of action exists under state law for the conduct complained of herein.

8. This Court has personal jurisdiction over Defendant because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in Illinois. The privacy violations complained of herein resulted from Defendant's purposeful and tortious acts directed towards citizens of Illinois while they were located within Illinois. At all relevant times, Defendant knew that its practices would directly result in collection of information from Illinois citizens while those citizens browse www.zillow.com. Defendant chose to avail itself of the business opportunities of making its real property and rental advertising services specifically available in Illinois (and specifically with respect to Illinois properties) and collecting real-time data from website visit sessions initiated by Illinoisans while located in Illinois, and the claims alleged herein arise from those activities.

9. Zillow also knows that many users visit and interact with Zillow's websites while they are physically present in Illinois. Both desktop and mobile versions of Zillow's website allow a user to search for nearby properties by providing the user's "current location," as furnished by the location-determining tools of the device the user is using or by the user's IP address (*i.e.*, without requiring the user to manually input an address). Users' employment of automatic location services in this way means that Zillow is continuously made aware that its website is being visited

by people located in Illinois, and that such website visitors are being eavesdropped on in violation of Illinois statutory and common law.

10. Pursuant to 735 ILCS 5/1-108, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District. Further, the sole defendant does not reside in Illinois and, accordingly, pursuant to 735 ILCS 5/2-101, this action may be brought in any Illinois county.

FACTUAL ALLEGATIONS

A. Website User and Usage Data Have Immense Economic Value.

11. The “world’s most valuable resource is no longer oil, but data.”¹

12. Earlier this year, Business News Daily reported that some businesses collect personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data (*i.e.*, how consumers interact with a business’s website, applications, and emails), behavioral data (*i.e.*, customers’ purchase histories and product usage information), and attitudinal data (*i.e.*, data on consumer satisfaction) from consumers.² This information is valuable to companies because they can use this data to improve customer experiences, refine their marketing strategies, capture data to sell it, and even to secure more sensitive consumer data.³

13. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business’s success.

¹ *The world’s most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

² Max Freedman, *How Businesses Are Collecting Data (And What They’re Doing With It)*, Business News Daily (Aug. 5, 2022), <https://www.businessnewsdaily.com/10625-businesses-collecting-data.html>.

³ *Id.*

Research shows that organizations who “leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin.”⁴

14. In 2013, the Organization for Economic Cooperation and Development (“OECD”) even published a paper entitled “Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value.”⁵ In this paper, the OECD measured prices demanded by companies concerning user data derived from “various online data warehouses.”⁶

15. OECD indicated that “[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e. \$2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver’s license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55.”⁷

B. Website Users Have a Reasonable Expectation of Privacy in Their Interactions with Websites.

16. Consumers are skeptical and are wary about their data being collected. A report released by KPMG shows that “a full 86% of the respondents said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected.”⁸

⁴ Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), <https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data>.

⁵ Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), <https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf>.

⁶ *Id.* at 25.

⁷ *Id.*

⁸ Lance Whitney, *Data privacy is a growing concern for more consumers*, TechRepublic (Aug. 17, 2021), <https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/>.

17. Another recent paper also indicates that most website visitors will assume their detailed interactions with a website will only be used by the website and not be shared with a party they know nothing about.⁹ As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.¹⁰

18. Privacy polls and studies show that a majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

19. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.¹¹

20. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.¹²

21. Users act consistently with their expectation of privacy. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing

⁹ *CUJO AI Recent Survey Reveals U.S. Internet Users Expectations and Concerns Towards Privacy and Online Tracking*, CUJO (May 26, 2020), <https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html>.

¹⁰ Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, *The Information Society*, 38:4, 257, 258 (2022).

¹¹ *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, *Consumer Reports* (May 11, 2017), <https://www.consumerreports.org/consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/>.

¹² *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, *Pew Research Center*, (Nov. 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confusedand-feeling-lack-of-control-over-their-personal-information/>.

companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.¹³

C. How Session Replay Code Works.

22. Session Replay Code, such as that implemented on www.zillow.com, enables website operators to record, save, and replay website visitors' interactions with a given website. The clandestinely deployed code provides online marketers and website designers with insights into the user experience by recording website visitors "as they click, scroll, type or navigate across different web pages."¹⁴

23. While Session Replay Code is utilized by websites for some legitimate purposes, it goes well beyond normal website analytics when it comes to collecting the actual contents of communications between website visitors and websites. Unlike other online advertising tools, Session Replay Code allows a website to capture and record nearly every action a website visitor takes while visiting the website, including actions that reveal the visitor's personal or private sensitive data, sometimes even when the visitor does not intend to submit the data to the website operator, or has not finished submitting the data to the website operator.¹⁵ As a result, website visitors "aren't just sharing data with the [web]site they're on . . . but also with an analytics service that may be watching over their shoulder."¹⁶

¹³ Margaret Taylor, *How Apple screwed Facebook*, *Wired*, (May 19, 2021), <https://www.wired.co.uk/article/apple-ios14-facebook>.

¹⁴ Erin Gilliam Haije, *[Updated] Are Session Recording Tools a Risk to Internet Privacy?*, *Mopinion* (Mar. 7, 2018), <https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/>.

¹⁵ *Id.*

¹⁶ Eric Ravenscraft, *Almost Every Website You Visit Records Exactly How Your Mouse Moves*, *Medium* (Feb. 5, 2020), <https://onezero.medium.com/almost-every-website-you-visit-records-exactly-how-your-mouse-moves-4134cb1cc7a0>.

24. Session Replay Code works by inserting computer code into the various event handling routines that web browsers use to receive input from users, thus intercepting the occurrence of actions the user takes. When a website delivers Session Replay Code to a user's browser, the browser will follow the code's instructions by sending responses in the form of "event" data to a designated third-party server. Typically, the server receiving the event data is controlled by the third-party entity that wrote the Session Replay Code, rather than the owner of the website where the code is installed.

25. The types of events captured by Session Replay Code vary by specific product and configuration, but in general are wide-ranging and can encompass virtually every user action, including all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entry, and numerous other forms of a user's navigation and interaction through the website. In order to permit a reconstruction of a user's visit accurately, the Session Replay Code must be capable of capturing these events at hyper-frequent intervals, often just milliseconds apart. Events are typically accumulated and transmitted in blocks periodically throughout the user's website session, rather than after the user's visit to the website is completely finished.

26. Unless specifically masked through configurations chosen by the website owner, some visible contents of the website may also be transmitted to the Session Replay Provider.

27. Once the events from a user session have been recorded by a Session Replay Code, a website operator can view a visual reenactment of the user's visit through the Session Replay Provider, usually in the form of a video, meaning "[u]nlike typical analytics services that provide

aggregate statistics, these scripts are intended for the recording and playback of individual browsing sessions.”¹⁷

28. Because most Session Replay Codes will by default indiscriminately capture the maximum range of user-initiated events and content displayed by the website, researchers have found that a variety of highly sensitive information can be captured in event responses from website visitors, including medical conditions, credit card details, and other personal information displayed or entered on webpages.¹⁸

29. Most alarming, Session Replay Code may capture data that the user did not even intentionally transmit to a website during a visit, and then make that data available to website owners when they access the session replay through the Session Replay Provider. For example, if a user writes information into a text form field, but then chooses not to click a “submit” or “enter” button on the website, the Session Replay Code may nevertheless cause the non-submitted text to be sent to the designated event-response-receiving server before the user deletes the text or leaves the page. This information will then be viewable to the website owner when accessing the session replay through the Session Replay Provider.

30. Session Replay Code does not necessarily anonymize user sessions, either.

31. First, if a user’s entry of personally identifying information is captured in an event response, that data will become known and visible to both the Session Replay Provider and the website owner.

¹⁷ Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), <https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/>.

¹⁸ *Id.*

32. Second, if a website displays user account information to a logged-in user, that content may be captured by Session Replay Code.

33. Third, some Session Replay Providers explicitly offer website owners cookie functionality that permits linking a session to an identified user, who may be personally identified if the website owner has associated the user with an email address or username.¹⁹

34. Session Replay Providers often create “fingerprints” that are unique to a particular user’s combination of computer and browser settings, screen configuration, and other detectable information. The resulting fingerprint, which is often unique to a user and rarely changes, are collected across all sites that the Session Replay Provider monitors.

35. When a user eventually identifies themselves to one of these websites (such as by filling in a form), the provider can then associate the fingerprint with the user identity and can then back-reference all of that user’s other web browsing across other websites previously visited, including on websites where the user had intended to remain anonymous—even if the user explicitly indicated that they would like to remain anonymous by enabling private browsing.

36. In addition to the privacy invasions caused by the diversion of user communications with websites to third-party Session Replay Providers, Session Replay Code also exposes website visitors to identity theft, online scams, and other privacy threats.²⁰ Indeed, “[t]he more copies of sensitive information that exist, the broader the attack surface, and when data is being collected [

¹⁹ *Id.*; see also *FS.identify – Identifying users*, FullStory, <https://help.fullstory.com/hc/en-us/articles/360020828113>, (last visited Sep. 8, 2022).

²⁰ Juha Sarrinen, *Session Replay is a Major Threat to Privacy on the Web*, itnews (Nov. 16, 2017), <https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720>.

] it may not be stored properly or have standard protections” increasing “the overall risk that data will someday publicly leak or be breached.”²¹

37. Recognizing the privacy concerns posed by Session Replay Code, in 2019 Apple required app developers to remove or properly disclose the use of analytics code that allow app developers to record how a user interacts with their iPhone apps or face immediate removal from the app store.²² In announcing this decision, Apple stated: “Protecting user privacy is paramount in the Apple ecosystem. Our App Store Review Guidelines require that apps request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity.”²³

D. Zillow Secretly Eavesdrops on its Website Visitors’ Electronic Communications.

38. Zillow operates the website www.zillow.com. Zillow is the “leading online residential real estate” marketplace in the United States for consumers, connecting them to the information and real estate professionals they need to buy, sell, or rent a home.²⁴

39. Zillow has become “synonymous with residential real estate.”²⁵ www.zillow.com is the most popular real estate website in the United States, with over thirty-six million unique

²¹ Lily Hay Newman, *Covert ‘Replay Sessions’ Have Been harvesting Passwords by Mistake*, WIRED (Feb. 26, 2018), <https://www.wired.com/story/covert-replay-sessions-harvesting-passwords/>.

²² Zack Whittaker, *Apple Tells App Developers to Disclose or Remove Screen Recording Code*, TechCrunch (Feb. 7, 2019), <https://techcrunch.com/2019/02/07/apple-glassbox-apps/>.

²³ *Id.*

²⁴ Zillow Group, Inc., *Form 10-K* (Dec. 31, 2021), <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001617640/87bbbf30-39cb-4eb7-acdc-1b51265b9687.pdf> (“Zillow 10-K”).

²⁵ *Id.*

monthly visitors²⁶ and more than 135 million properties are listed on its website.²⁷ According to a 2021 Google Trends report, “[t]oday more people search ‘Zillow’ than ‘real estate.’”²⁸

40. However, unbeknownst to the millions of individuals perusing Zillow’s real estate listings, Zillow knowingly directs Session Replay Providers to embed various Session Replay Codes on its website to track and analyze website user interactions with www.zillow.com. Because the Session Replay Providers are unknown eavesdroppers to visitors to www.zillow.com, they are not parties to website visitors’ Website Communications with Zillow.

41. One such Session Replay Provider that Zillow procures is Microsoft.

42. Microsoft is the owner and operator of a Session Replay Code titled Clarity, which provides basic information about website user sessions, interactions, and engagement, and breaks down users by device type, county, and other dimensions.²⁹

43. Zillow knowingly derives a benefit and/or information from the Website Communications intercepted and recorded at its direction. Upon information and belief, Zillow uses the intercepted Website Communications to replay website visitors’ interactions with www.zillow.com, improve user interactions with its website, and to provide targeted real estate advertisements to its website visitors.

44. Zillow’s knowing direction and use of Microsoft Clarity’s Session Replay Code, direction and use of other Session Replay Codes through various Session Replay Providers, and its knowing derivation of a benefit and/or information from the Website Communications

²⁶ *Most Popular Real Estate Websites in the United States as of October 2021, Based on Unique Monthly Visits*, Statista, <https://www.statista.com/statistics/381468/most-popular-real-estate-websites-by-monthly-visits-usa/>, (last visited Sep. 8, 2022).

²⁷ Zillow 10-K, *supra*, note 1.

²⁸ *Id.*

²⁹ Jono Alderson, *An Introduction to Microsoft Clarity*, Yoast, <https://yoast.com/introduction-microsoft-clarity/#h-what-is-microsoft-clarity>, (last visited Sep. 8, 2022).

surreptitiously intercepted and recorded by Session Replay Codes is a violation of Illinois statutory and common law.

E. Plaintiff's and Class Members' Experience.

45. Plaintiff has visited www.zillow.com on her computer while in Illinois.

46. While visiting Zillow's website, Plaintiff fell victim to Defendant's unlawful monitoring, recording, and collection of Plaintiff's Website Communications with www.zillow.com.

47. Unknown to Plaintiff, Zillow directs Session Replay Providers to embed Session Replay Code on its website.

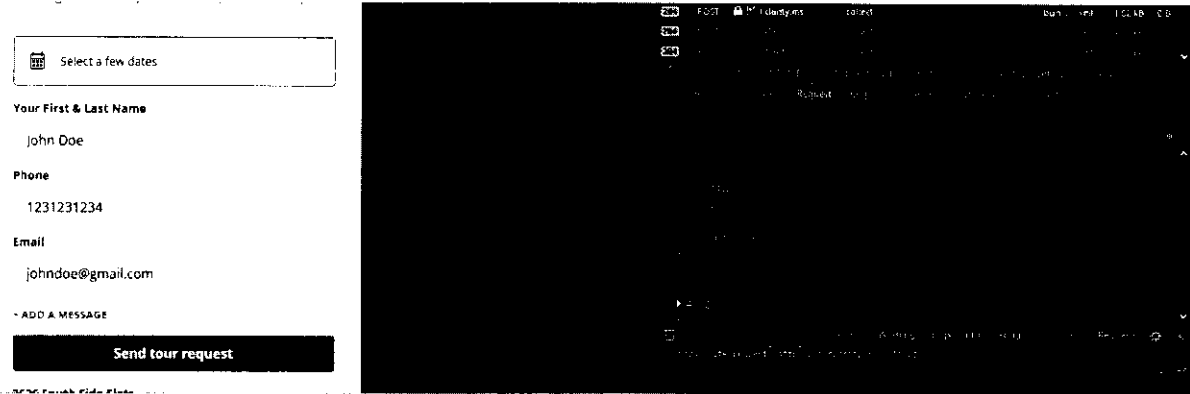
48. During the website visit, Plaintiff's Website Communications were captured by Session Replay Code and sent to various Session Replay Providers.

49. For example, when visiting www.zillow.com, if a website user views a certain piece of property for rent or sale, that information is captured by the Session Replay Codes embedded on the website:



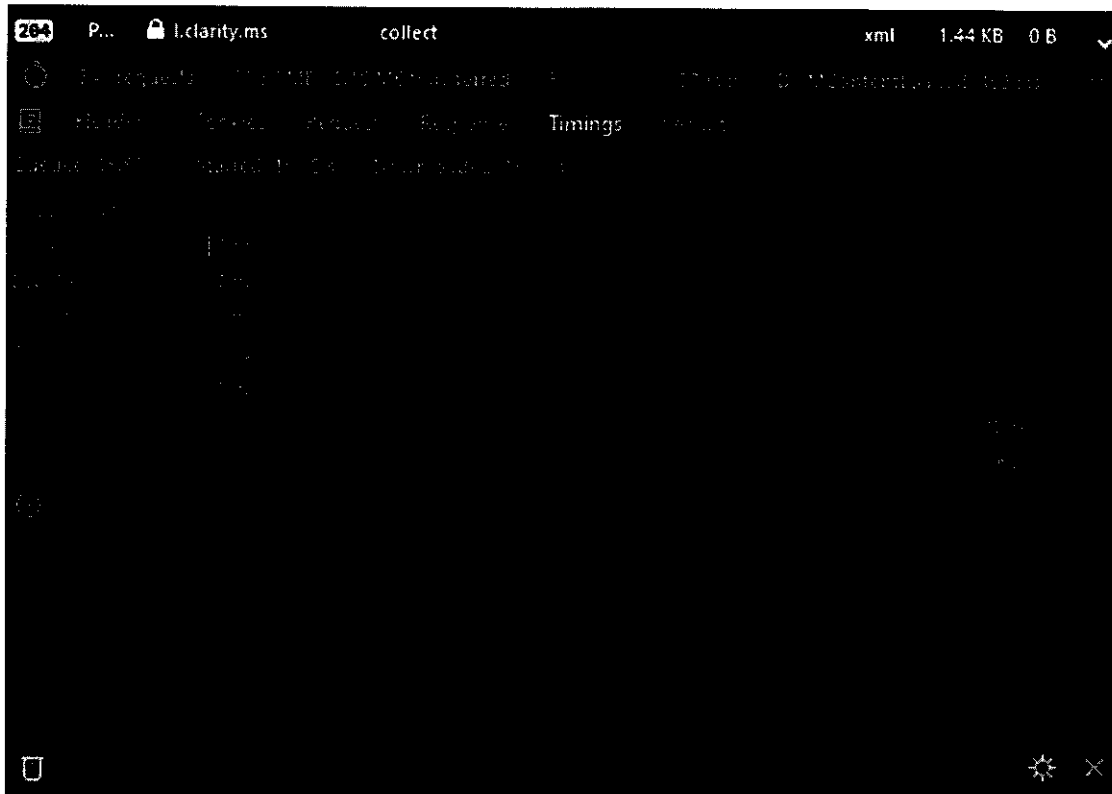
Depicting information sent to one of the Service Replay Providers—Microsoft—through a Service Replay Code—Clarity—after viewing a Studio apartment priced at \$1,488 while visiting www.zillow.com.

50. Similarly, when visiting www.zillow.com, if a user enters personal information in a text box to schedule a tour, that information is captured by the Session Replay Codes embedded on the website:



Depicting information sent to one of the Service Replay Providers—Microsoft—through a Service Replay Code—Clarity—after entering a name (purple text) to a text box to schedule a tour of a property.

51. The eavesdropping by the Session Replay Code is ongoing during the visit and they intercept the contents of these communications between Plaintiff and Zillow with instantaneous transmissions to the Session Replay Providers, as illustrated below, in which only 30 milliseconds were required to send a packet of even response data, which would indicate whatever the website user had just done:



52. The Session Replay Codes operate in the same manner for all putative Class members.

53. Like Plaintiff, each Class member visited www.zillow.com with Session Replay Code embedded in it, and those Session Replay Codes intercepted the Class members' Website Communications with www.zillow.com by sending hyper-frequent logs of those communications to Session Replay Providers.

54. Even if Zillow masks certain elements when it configures the settings of the Session Replay Code embedded on its website, any operational iteration of the Session Replay Code will, by its very nature and purpose, intercept the contents of communications between the website's visitors and the website owner.

55. For example, even with heightened masking enabled, Session Replay Providers will still learn through the intercepted data exactly which pages a user navigates to, how the user moves

through the page (such as which areas the user zooms in on or interacted with), and additional substantive information.

56. As a specific example, if a user types a particular address or zip code into Zillow's main search bar and initiates a search, even if the text entered into the search bar is masked, Session Replay Providers will still learn what is entered into the bar as soon as the search result page loads. This is so because the responsive search results will be displayed on the subsequent page, and the responsive content generated by Zillow will repeat the searched information back on the generated page. That information will not be masked even if user-inputted text is fully masked in a text field.

CLASS ACTION ALLEGATIONS

57. Plaintiff brings this action pursuant to 735 ILCS 5/2-801, individually and on behalf of the following Class:

All natural persons in the State of Illinois whose Website Communications were captured through the use of Session Replay Code embedded in www.zillow.com.

58. Excluded from the class are Defendant, its parents, subsidiaries, affiliates, officers, and directors, all persons who make a timely election to be excluded from the class, the judge to whom this case is assigned and any immediate family members thereof, and the attorneys who enter their appearance in this action.

59. **Numerosity:** The members of the Class are so numerous that individual joinder of all Class members is impracticable. The precise number of Class members and their identities may be obtained from the books and records of Zillow or the Session Replay Providers.

60. **Commonality:** This action involves questions of law and fact that are common to the Class members. Such common questions include, but are not limited to: (a) whether Defendant employed Session Replay Providers to intercept and record Zillow's website visitors' Website Communications; (b) whether Defendant operated or participated in the operation of an

eavesdropping device; (c) whether Defendant derives a benefit or information from the illegal use of an eavesdropping device; (d) whether Defendant directed another to use an eavesdropping device illegally on its behalf; (e) whether Session Replay Code is an “eavesdropping device” used to intercept or record private electronic communications; (f) whether Defendant acquired the contents of website users’ private electronic communications without their consent; (g) whether Plaintiff and Class members had a reasonable expectation of privacy in their Website communications; (f) whether Defendant violated the Illinois Eavesdropping Act 720 ILCS 5/14-1, *et seq.*; (g) whether Defendant’s interception of Plaintiff’s and Class members’ private electronic communications is an unfair or deceptive act or practice; (h) whether Zillow’s conduct violates the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.* (i) whether Plaintiff and the Class members are entitled to equitable relief; and (j) whether Plaintiff and the Class members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

61. **Typicality:** Plaintiff’s claims are typical of the other Class members’ claims because, among other things, all Class members were comparably injured through the uniform prohibited conduct described above. For instance, Plaintiff and each member of the Class had their electronic communications intercepted in violation of the law and their right to privacy. This uniform injury and the legal theories that underpin recovery make the claims of Plaintiff and the members of the Class typical of one another.

62. **Adequacy of Representation:** Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiff has no interest that is antagonistic to the interests of the Class, and Defendant

has no defenses unique to any Plaintiff. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiff nor her counsel have any interest adverse to the interests of the other members of the Class.

63. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

64. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant intercepted Plaintiff's and Class members' Website Communications, then Plaintiff and each Class member suffered damages by that conduct.

65. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class members may be readily identified through Zillow's books and records or the Session Replay Providers' books and records.

COUNT I
Violation of Illinois Eavesdropping Act
720 ILCS 5/14-1, *et seq.*

66. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

67. Plaintiff brings this claim individually and on behalf of the Class.

68. The Illinois Eavesdropping Act (the “Act”) prohibits (1) using an eavesdropping device in a surreptitious manner to overhear, transmit, or record all or any part of any private conversation; (2) intercepting, recording, or transcribing, in a surreptitious manner, any private electronic communication without consent; (3) manufacturing, assembling, distributing, or possessing any electronic, mechanical, eavesdropping, or other device knowing that or having reason to know that the design of the device renders it primarily useful for the purpose of surreptitious overhearing, transmitting, or recording of private conversations or the intersection; or (4) using or disclosing any information which he or she knows or reasonably should know was obtained from a private conversation or private electronic communication without the consent of all parties to the private electronic communication. 720 ILCS 5/14-2.

69. Any party to any conversation or private electronic communication upon which eavesdropping was practiced shall be entitled to (1) an injunction to prohibit further eavesdropping; (2) actual damages; and (3) punitive damages. punitive damages; 720 ILCS 5/14-6.

70. “Eavesdropping device” is defined as any “any device capable of being used to hear or record oral conversation or intercept, or transcribe electronic communications whether such conversation or electronic communication is conducted in person, by telephone, or by any other means[.]” 720 ILCS 5/14-1(a).

71. “Eavesdropper” is defined as “any person, including any law enforcement officer and any party to a private conversation, who operates or participates in the operation of any eavesdropping device contrary to the provisions of this Article or who acts as a principal, as defined in this Article.” 720 ILCS 5/14-1(b).

72. “Principle” is defined as “any person who: (1) knowingly employs another who illegally uses an eavesdropping device in the course of such employment; or (2) knowingly derives any benefit or information from the illegal use of an eavesdropping device by another; or (3) directs another to use an eavesdropping device illegally on his or her behalf.” 720 ILCS 5/14-1(c).

73. “Private electronic communication” is defined as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation. A reasonable expectation shall include any expectation recognized by law, including, but not limited to, an expectation derived from a privilege, immunity, or right established by common law, Supreme Court rule, or the Illinois or United States Constitution.” ILCS 5/14-1(e).

74. “Surreptitious” is defined as being “obtained or made by stealth or deception, or executed through secrecy or concealment.” 720 ILCS 5/14-1(g).

75. Zillow is an “Eavesdropper” and “Principal” for purposes of the Act because it operates or participates in the operation of an eavesdropping device, knowingly employs another who illegally uses an eavesdropping device, derives a benefit or information from the illegal use of an eavesdropping device, and directs another to use an eavesdropping device illegally on its behalf.

76. Session Replay Code like that operated and employed at Zillow’s direction is a “eavesdropping device” used to transcribe electronic communications within the meaning of the Act.

77. The Session Replay Providers are not a party to the Website Communications—Plaintiff and the Class only knew they were communicating with Zillow, not the Session Replay Providers.

78. Plaintiff's and Class members' intercepted Website Communications constitute the private electronic communications and private conversations within the meaning of the Act.

79. Zillow intentionally operated and employed Session Replay Code on its website to spy on, automatically and secretly, and intercept its website visitors' private electronic interactions communications with Zillow in real time.

80. Plaintiff's and Class members' private electronic communications were intercepted contemporaneously with their transmission.

81. Plaintiff and Class members had a reasonable expectation of privacy in their Website Communications based on the detailed information the Session Replay Code collected from Plaintiff and Class members.

82. Plaintiff and Class members did not consent to having their Website Communications surreptitiously intercepted and recorded.

83. Pursuant to 720 ILCS 5/14-6, Plaintiff and members of the Class are entitled to: (1) an injunction to prohibit further eavesdropping; (2) actual damages; and (3) punitive damages.

84. Zillow's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT II

**Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act
815 ILCS 505/1 *et seq.***

85. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

86. Plaintiff brings this claim individually and on behalf of the Class.

87. The Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.* (“ICFA”) protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

88. The ICFA prohibits “unfair or deceptive acts or practices,” including “misrepresentation or the concealment, suppression or omission of any material fact.” 815 ILCS 505/2.

89. The ICFA applies to Zillow’s conduct described herein because it protects consumers in transactions that are intended to result, or which have resulted in the sale of goods or services.

90. Zillow is a “person” within the meaning of ILCS 505/1(c) because it is a corporation.

91. Plaintiff and members of the Class are “consumers” within the meaning of 815 ILCS 505/1(e) because they visited www.zillow.com to shop for, purchase, or contract to purchase “merchandise”—real estate—for their own use.

92. Zillow’s advertising, offering for sale, and sale of real estate on www.zillow.com is considered “trade” or “commerce” within the meaning of 815 ILCS 505/1(f).

93. Zillow violated the ICFA by concealing material facts about www.zillow.com. Specifically, Zillow omitted and concealed that it directed Session Replay Providers to secretly

monitor, collect, transmit, and discloses its website visitors' Website Communications to the Session Replay Providers using Session Replay Code.

94. Zillow's direction and employment of the Session Replay Providers and their Session Replay Codes to intercept, collect, and disclose website visitors' Website Communications are material to the transactions on www.zillow.com. Zillow is leading online residential real estate marketplace in the United States and Zillow does not disclose its use of Session Replay Code to secretly monitor and collect website visitors' Website Communications. Had Plaintiff and the Class members known that the Session Replay Codes (that collect, transmit, and disclose Website Communications to the Session Replay Providers) were embedded in Zillow's website, they would not have visited www.zillow.com to shop for, purchase, or contract to purchase real estate or they would have required Zillow to compensate them for the interception, collection, and disclosure of their Website Communications.

95. Zillow's intentional concealment of the interception, collection, and disclosure of website visitors' Website Communications using Session Replay Code embedded in www.zillow.com is material because it knows that consumers would not otherwise visit its website to search for, purchase, and contract to purchase real estate. Indeed, Zillow's concealment of such facts was intended to mislead consumers.

96. Zillow's concealment, suppression, and omission of material facts was likely to mislead reasonable consumers under the circumstances, and thus constitutes an unfair and deceptive trade practice in violation of the ICFA.

97. By failing to disclose and inform Plaintiff and the Class about its interception, collection, and disclosure of website visitors' Website Communications, Zillow violated section 505/2 of the ICFA.

98. As a direct and proximate result of these unfair and deceptive practices, Plaintiff and each Class member has suffered actual harm in the form of money and/or property because the disclosure of their Website Communications has value as demonstrated by the collection and use of it by Zillow. The collection and use of this information has now diminished the value of such information to Plaintiff and the Class.

99. As such, Plaintiff and the Class seek an order (1) requiring Zillow to cease the unfair practices described herein; (2) awarding actual damages; and (3) awarding reasonable attorneys' fees and costs.

100. Zillow's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT III **Invasion of Privacy – Intrusion Upon Seclusion**

101. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

102. Illinois common law recognizes the tort of invasion of privacy. The right to privacy is also embodied in the Illinois constitution.

103. Plaintiff brings this claim individually and on behalf of the Class.

104. Plaintiff and Class members had an objective, reasonable expectation of privacy in their Website Communications.

105. Plaintiff and Class members did not consent to, authorize, or know about Zillow's intrusion at the time it occurred. Plaintiff and Class members never agreed that Zillow could collect or disclose their Website Communications.

106. Plaintiff and Class members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

107. Zillow intentionally intruded on Plaintiff's and Class members' private life, seclusion, or solitude, without consent.

108. Zillow's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

109. Plaintiff and Class members were harmed by Zillow's wrongful conduct as Zillow's conduct has caused Plaintiff and the Class mental anguish and suffering arising from their loss of privacy and confidentiality of their electronic communications.

110. Zillow's conduct has needlessly harmed Plaintiff and the Class by capturing intimately personal facts and data in the form of their Website Communications. This disclosure and loss of privacy and confidentiality has caused Plaintiff and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

111. Additionally, given the monetary value of individual personal information, Defendant deprived Plaintiff and Class members of the economic value of their interactions with Defendant's website, without providing proper consideration for Plaintiff's and Class members' property.

112. Further, Zillow has improperly profited from its invasion of Plaintiff and Class members' privacy in its use of their data for its economic value.

113. As a direct and proximate result Zillow's conduct, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

114. Zillow's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with session replay software enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

REQUEST FOR RELIEF

Plaintiff, individually and on behalf of the other members of the proposed Class, respectfully requests that the Court enter judgment in Plaintiff's and the Class's favor and against Defendant as follows:

- A. Certifying the Class and appointing Plaintiff as the Class representative;
- B. Appointing Plaintiff's counsel as class counsel;
- C. Declaring that Defendant's past conduct was unlawful, as alleged herein;
- D. Declaring Defendant's ongoing conduct is unlawful, as alleged herein;
- E. Enjoining Defendant from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;
- F. Awarding Plaintiff and the Class members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;
- G. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

H. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

I. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the Class, demands a trial by jury of any and all issues in this action so triable of right.

Dated: September 15, 2022

Respectfully submitted,

BY: /s/ Katrina Carroll
LYNCH CARPENTER, LLP
KATRINA CARROLL
KYLE SHAMBERG
111 W. Washington Street
Suite 1240
Chicago, IL 60602
Office: 312.750.1265
Fax: 773.598.5609
katrina@lcllp.com
kyle@lcllp.com

GARY LYNCH
LYNCH CARPENTER LLP
1133 Penn Avenue
5th Floor
Pittsburgh, PA 15222
Office: 412.322.9243
Fax: 412.231.0246
gary@lcllp.com

Exhibit B

**CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT – CHANCERY DIVISION**

JILL STRELZIN, individually and on)
behalf of all others similarly situated,)
)
Plaintiff,)
)
vs.) Case No. 2022CH09132
)
ZILLOW GROUP, INC.,)
)
Defendant.)
)

NOTICE OF FILING OF REMOVAL

TO THE CLERK:

PLEASE TAKE NOTICE that Defendant Zillow Group, Inc. filed a Notice of Removal on October 14, 2022, in the United States District Court for the Northern District of Illinois, a copy of which is attached as Exhibit A. Pursuant to 28 U.S.C. § 1446(d), the filing of this Notice effects the removal of this case, and this Court shall proceed no further unless the case is remanded.

Respectfully submitted,

Dated: October 14, 2022

BUCHANAN INGERSOLL & ROONEY PC

By: /s/ David T. Cellitti

David T. Cellitti (Bar No. 6272041)
401 E. Jackson Street, Suite 2400
Tampa, FL 33602
Tel. 813-222-8180
david.cellitti@bipc.com

Counsel for Defendant Zillow Group, Inc.

Exhibit C

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS**

RYAN MARGULIS, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

ZILLOW GROUP, INC.,

Defendant.

Case No. _____

JURY TRIAL DEMANDED

COMPLAINT - CLASS ACTION

Plaintiff Ryan Margulis (“Plaintiff”), individually and on behalf of all others similarly situated, hereby files this class action complaint against Defendant Zillow Group, Inc. (“Defendant” or “Zillow”), and in support thereof alleges the following:

INTRODUCTION

1. This is a class action brought against Zillow for surreptitiously intercepting the private electronic communications of visitors to its website, www.zillow.com, without their consent. Zillow knowingly directs third-party vendors, such as Microsoft Corporation, to embed snippets of JavaScript computer code (“Session Replay Code”) on Zillow’s website, which then deploys on each website visitor’s internet browser for the purpose intercepting and recording the website visitor’s private electronic communications with the Zillow website, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time (“Website Communications”). These third-party vendors (collectively, “Session Replay Providers”) create and deploy the Session Replay Code at Zillow’s request.

2. After intercepting and recording the Website Communications, Zillow and the Session Replay Providers use those Website Communications to recreate website visitors' entire visit to www.zillow.com. The Session Replay Providers create a video replay of the user's behavior on the website and provide it to Zillow for analysis. Zillow's directive to the Session Replay Providers to secretly deploy the Session Replay Code results in the electronic equivalent of "looking over the shoulder" of each visitor to the Zillow website for the entire duration of their website interaction.

3. Zillow's conduct violates the Illinois Eavesdropping Act, 720 ILCS 5/14-1, *et seq.*, the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.*, and constitutes an invasion of the privacy rights of website visitors.

4. Plaintiff brings this action individually and on behalf of a class of all Illinois citizens whose Website Communications were intercepted at Zillow's direction and use of Session Replay Code embedded on the webpages of www.zillow.com and seeks all civil remedies provided under the causes of action, including but not limited to compensatory, statutory, and/or punitive damages, and attorneys' fees and costs.

PARTIES

5. Plaintiff Ryan Margulis is a citizen of the state of Illinois, and at all times relevant to this action, resided and was domiciled in Cook county, Illinois. Plaintiff is a citizen of Illinois.

6. Defendant Zillow Group, Inc. is corporation organized under the laws of Washington, and its principal place of business is located at 1301 Second Ave., Floor 31, Seattle Washington, 98101. Defendant is a citizen of Washington.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of \$5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class, including Plaintiff, is a citizen of a state different than Defendant.

8. This Court has personal jurisdiction over Defendant because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in Illinois. The privacy violations complained of herein resulted from Defendant's purposeful and tortious acts directed towards citizens of Illinois while they were located within Illinois. At all relevant times, Defendant knew that its practices would directly result in collection of information from Illinois citizens while those citizens browse www.zillow.com. Defendant chose to avail itself of the business opportunities of making its real property and rental advertising services specifically available in Illinois (and specifically with respect to Illinois properties) and collecting real-time data from website visit sessions initiated by Illinoisans while located in Illinois, and the claims alleged herein arise from those activities.

9. Zillow also knows that many users visit and interact with Zillow's websites while they are physically present in Illinois. Both desktop and mobile versions of Zillow's website allow a user to search for nearby properties by providing the user's "current location," as furnished by the location-determining tools of the device the user is using or by the user's IP address (*i.e.*, without requiring the user to manually input an address). Users' employment of automatic location services in this way means that Zillow is continuously made aware that its website is being visited

by people located in Illinois, and that such website visitors are being eavesdropped on in violation of Illinois statutory and common law.

10. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

FACTUAL ALLEGATIONS

A. Website User and Usage Data Have Immense Economic Value.

11. The “world’s most valuable resource is no longer oil, but data.”¹

12. Earlier this year, Business News Daily reported that some businesses collect personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data (*i.e.*, how consumers interact with a business’s website, applications, and emails), behavioral data (*i.e.*, customers’ purchase histories and product usage information), and attitudinal data (*i.e.*, data on consumer satisfaction) from consumers.² This information is valuable to companies because they can use this data to improve customer experiences, refine their marketing strategies, capture data to sell it, and even to secure more sensitive consumer data.³

13. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business’s success.

¹ *The world’s most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

² Max Freedman, *How Businesses Are Collecting Data (And What They’re Doing With It)*, Business News Daily (Aug. 5, 2022), <https://www.businessnewsdaily.com/10625-businesses-collecting-data.html>.

³ *Id.*

Research shows that organizations who “leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin.”⁴

14. In 2013, the Organization for Economic Cooperation and Development (“OECD”) even published a paper entitled “Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value.”⁵ In this paper, the OECD measured prices demanded by companies concerning user data derived from “various online data warehouses.”⁶

15. OECD indicated that “[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e. \$2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver’s license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55.”⁷

B. Website Users Have a Reasonable Expectation of Privacy in Their Interactions with Websites.

16. Consumers are skeptical and are wary about their data being collected. A report released by KPMG shows that “a full 86% of the respondents said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected.”⁸

⁴ Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), <https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data>.

⁵ Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), <https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf>.

⁶ *Id.* at 25.

⁷ *Id.*

⁸ Lance Whitney, *Data privacy is a growing concern for more consumers*, TechRepublic (Aug. 17, 2021), <https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/>.

17. Another recent paper also indicates that most website visitors will assume their detailed interactions with a website will only be used by the website and not be shared with a party they know nothing about.⁹ As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.¹⁰

18. Privacy polls and studies show that a majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

19. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.¹¹

20. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.¹²

21. Users act consistently with their expectation of privacy. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing

⁹ *CUJO AI Recent Survey Reveals U.S. Internet Users Expectations and Concerns Towards Privacy and Online Tracking*, CUJO (May 26, 2020), <https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html>.

¹⁰ Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, *The Information Society*, 38:4, 257, 258 (2022).

¹¹ *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, Consumer Reports (May 11, 2017), <https://www.consumerreports.org/consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/>.

¹² *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, (Nov. 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confusedand-feeling-lack-of-control-over-their-personal-information/>.

companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.¹³

C. How Session Replay Code Works.

22. Session Replay Code, such as that implemented on www.zillow.com, enables website operators to record, save, and replay website visitors’ interactions with a given website. The clandestinely deployed code provides online marketers and website designers with insights into the user experience by recording website visitors “as they click, scroll, type or navigate across different web pages.”¹⁴

23. While Session Replay Code is utilized by websites for some legitimate purposes, it goes well beyond normal website analytics when it comes to collecting the actual contents of communications between website visitors and websites. Unlike other online advertising tools, Session Replay Code allows a website to capture and record nearly every action a website visitor takes while visiting the website, including actions that reveal the visitor’s personal or private sensitive data, sometimes even when the visitor does not intend to submit the data to the website operator, or has not finished submitting the data to the website operator.¹⁵ As a result, website visitors “aren’t just sharing data with the [web]site they’re on . . . but also with an analytics service that may be watching over their shoulder.”¹⁶

¹³ Margaret Taylor, *How Apple screwed Facebook*, Wired, (May 19, 2021), <https://www.wired.co.uk/article/apple-ios14-facebook>.

¹⁴ Erin Gilliam Haije, *[Updated] Are Session Recording Tools a Risk to Internet Privacy?*, Mopinion (Mar. 7, 2018), <https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/>.

¹⁵ *Id.*

¹⁶ Eric Ravenscraft, *Almost Every Website You Visit Records Exactly How Your Mouse Moves*, Medium (Feb. 5, 2020), <https://onezero.medium.com/almost-every-website-you-visit-records-exactly-how-your-mouse-moves-4134cb1cc7a0>.

24. Session Replay Code works by inserting computer code into the various event handling routines that web browsers use to receive input from users, thus intercepting the occurrence of actions the user takes. When a website delivers Session Replay Code to a user's browser, the browser will follow the code's instructions by sending responses in the form of "event" data to a designated third-party server. Typically, the server receiving the event data is controlled by the third-party entity that wrote the Session Replay Code, rather than the owner of the website where the code is installed.

25. The types of events captured by Session Replay Code vary by specific product and configuration, but in general are wide-ranging and can encompass virtually every user action, including all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entry, and numerous other forms of a user's navigation and interaction through the website. In order to permit a reconstruction of a user's visit accurately, the Session Replay Code must be capable of capturing these events at hyper-frequent intervals, often just milliseconds apart. Events are typically accumulated and transmitted in blocks periodically throughout the user's website session, rather than after the user's visit to the website is completely finished.

26. Unless specifically masked through configurations chosen by the website owner, some visible contents of the website may also be transmitted to the Session Replay Provider.

27. Once the events from a user session have been recorded by a Session Replay Code, a website operator can view a visual reenactment of the user's visit through the Session Replay Provider, usually in the form of a video, meaning "[u]nlike typical analytics services that provide

aggregate statistics, these scripts are intended for the recording and playback of individual browsing sessions.”¹⁷

28. Because most Session Replay Codes will by default indiscriminately capture the maximum range of user-initiated events and content displayed by the website, researchers have found that a variety of highly sensitive information can be captured in event responses from website visitors, including medical conditions, credit card details, and other personal information displayed or entered on webpages.¹⁸

29. Most alarming, Session Replay Code may capture data that the user did not even intentionally transmit to a website during a visit, and then make that data available to website owners when they access the session replay through the Session Replay Provider. For example, if a user writes information into a text form field, but then chooses not to click a “submit” or “enter” button on the website, the Session Replay Code may nevertheless cause the non-submitted text to be sent to the designated event-response-receiving server before the user deletes the text or leaves the page. This information will then be viewable to the website owner when accessing the session replay through the Session Replay Provider.

30. Session Replay Code does not necessarily anonymize user sessions, either.

31. First, if a user’s entry of personally identifying information is captured in an event response, that data will become known and visible to both the Session Replay Provider and the website owner.

¹⁷ Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), <https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/>.

¹⁸ *Id.*

32. Second, if a website displays user account information to a logged-in user, that content may be captured by Session Replay Code.

33. Third, some Session Replay Providers explicitly offer website owners cookie functionality that permits linking a session to an identified user, who may be personally identified if the website owner has associated the user with an email address or username.¹⁹

34. Session Replay Providers often create “fingerprints” that are unique to a particular user’s combination of computer and browser settings, screen configuration, and other detectable information. The resulting fingerprint, which is often unique to a user and rarely changes, are collected across all sites that the Session Replay Provider monitors.

35. When a user eventually identifies themselves to one of these websites (such as by filling in a form), the provider can then associate the fingerprint with the user identity and can then back-reference all of that user’s other web browsing across other websites previously visited, including on websites where the user had intended to remain anonymous—even if the user explicitly indicated that they would like to remain anonymous by enabling private browsing.

36. In addition to the privacy invasions caused by the diversion of user communications with websites to third-party Session Replay Providers, Session Replay Code also exposes website visitors to identity theft, online scams, and other privacy threats.²⁰ Indeed, “[t]he more copies of sensitive information that exist, the broader the attack surface, and when data is being collected [

¹⁹ *Id.*; see also *FS.identify – Identifying users*, FullStory, <https://help.fullstory.com/hc/en-us/articles/360020828113>, (last visited Sep. 8, 2022).

²⁰ Juha Sarrinen, *Session Replay is a Major Threat to Privacy on the Web*, itnews (Nov. 16, 2017), <https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720>.

] it may not be stored properly or have standard protections” increasing “the overall risk that data will someday publicly leak or be breached.”²¹

37. Recognizing the privacy concerns posed by Session Replay Code, in 2019 Apple required app developers to remove or properly disclose the use of analytics code that allow app developers to record how a user interacts with their iPhone apps or face immediate removal from the app store.²² In announcing this decision, Apple stated: “Protecting user privacy is paramount in the Apple ecosystem. Our App Store Review Guidelines require that apps request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity.”²³

D. Zillow Secretly Eavesdrops on its Website Visitors’ Electronic Communications.

38. Zillow operates the website www.zillow.com. Zillow is the “leading online residential real estate” marketplace in the United States for consumers, connecting them to the information and real estate professionals they need to buy, sell, or rent a home.²⁴

39. Zillow has become “synonymous with residential real estate.”²⁵ www.zillow.com is the most popular real estate website in the United States, with over thirty-six million unique

²¹ Lily Hay Newman, *Covert ‘Replay Sessions’ Have Been harvesting Passwords by Mistake*, WIRED (Feb. 26, 2018), <https://www.wired.com/story/covert-replay-sessions-harvesting-passwords/>.

²² Zack Whittaker, *Apple Tells App Developers to Disclose or Remove Screen Recording Code*, TechCrunch (Feb. 7, 2019), <https://techcrunch.com/2019/02/07/apple-glassbox-apps/>.

²³ *Id.*

²⁴ Zillow Group, Inc., *Form 10-K* (Dec. 31, 2021), <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001617640/87bbb30-39cb-4eb7-acdc-1b51265b9687.pdf> (“Zillow 10-K”).

²⁵ *Id.*

monthly visitors²⁶ and more than 135 million properties are listed on its website.²⁷ According to a 2021 Google Trends report, “[t]oday more people search ‘Zillow’ than ‘real estate.’”²⁸

40. However, unbeknownst to the millions of individuals perusing Zillow’s real estate listings, Zillow knowingly directs Session Replay Providers to embed various Session Replay Codes on its website to track and analyze website user interactions with www.zillow.com. Because the Session Replay Providers are unknown eavesdroppers to visitors to www.zillow.com, they are not parties to website visitors’ Website Communications with Zillow.

41. One such Session Replay Provider that Zillow procures is Microsoft.

42. Microsoft is the owner and operator of a Session Replay Code titled Clarity, which provides basic information about website user sessions, interactions, and engagement, and breaks down users by device type, county, and other dimensions.²⁹

43. Zillow knowingly derives a benefit and/or information from the Website Communications intercepted and recorded at its direction. Upon information and belief, Zillow uses the intercepted Website Communications to replay website visitors’ interactions with www.zillow.com, improve user interactions with its website, and to provide targeted real estate advertisements to its website visitors.

44. Zillow’s knowing direction and use of Microsoft Clarity’s Session Replay Code, direction and use of other Session Replay Codes through various Session Replay Providers, and its knowing derivation of a benefit and/or information from the Website Communications

²⁶ *Most Popular Real Estate Websites in the United States as of October 2021, Based on Unique Monthly Visits*, Statista, <https://www.statista.com/statistics/381468/most-popular-real-estate-websites-by-monthly-visits-usa/>, (last visited Sep. 8, 2022).

²⁷ Zillow 10-K, *supra*, note 1.

²⁸ *Id.*

²⁹ Jono Alderson, *An Introduction to Microsoft Clarity*, Yoast, <https://yoast.com/introduction-microsoft-clarity/#h-what-is-microsoft-clarity>, (last visited Sep. 8, 2022).

surreptitiously intercepted and recorded by Session Replay Codes is a violation of Illinois statutory and common law.

E. Plaintiff's and Class Members' Experience.

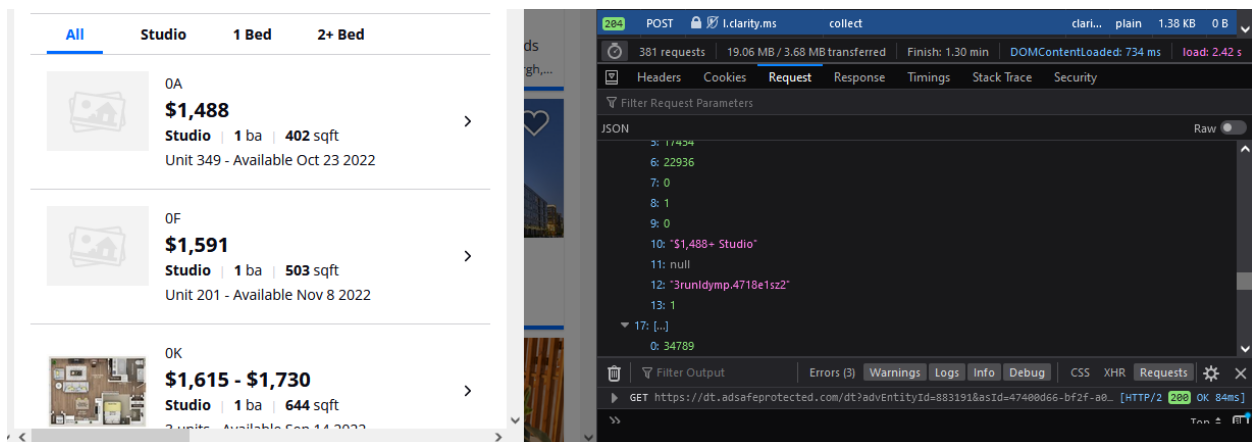
45. Plaintiff has visited www.zillow.com on his mobile devices and computer while in Illinois.

46. While visiting Zillow's website, Plaintiff fell victim to Defendant's unlawful monitoring, recording, and collection of Plaintiff's Website Communications with www.zillow.com.

47. Unknown to Plaintiff, Zillow directs Session Replay Providers to embed Session Replay Code on its website.

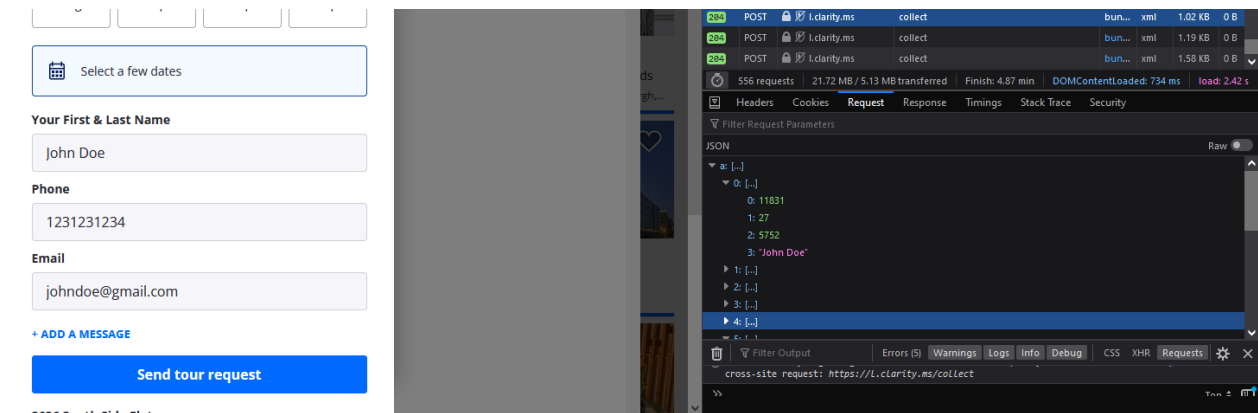
48. During the website visit, Plaintiff's Website Communications were captured by Session Replay Code and sent to various Session Replay Providers.

49. For example, when visiting www.zillow.com, if a website user views a certain piece of property for rent or sale, that information is captured by the Session Replay Codes embedded on the website:



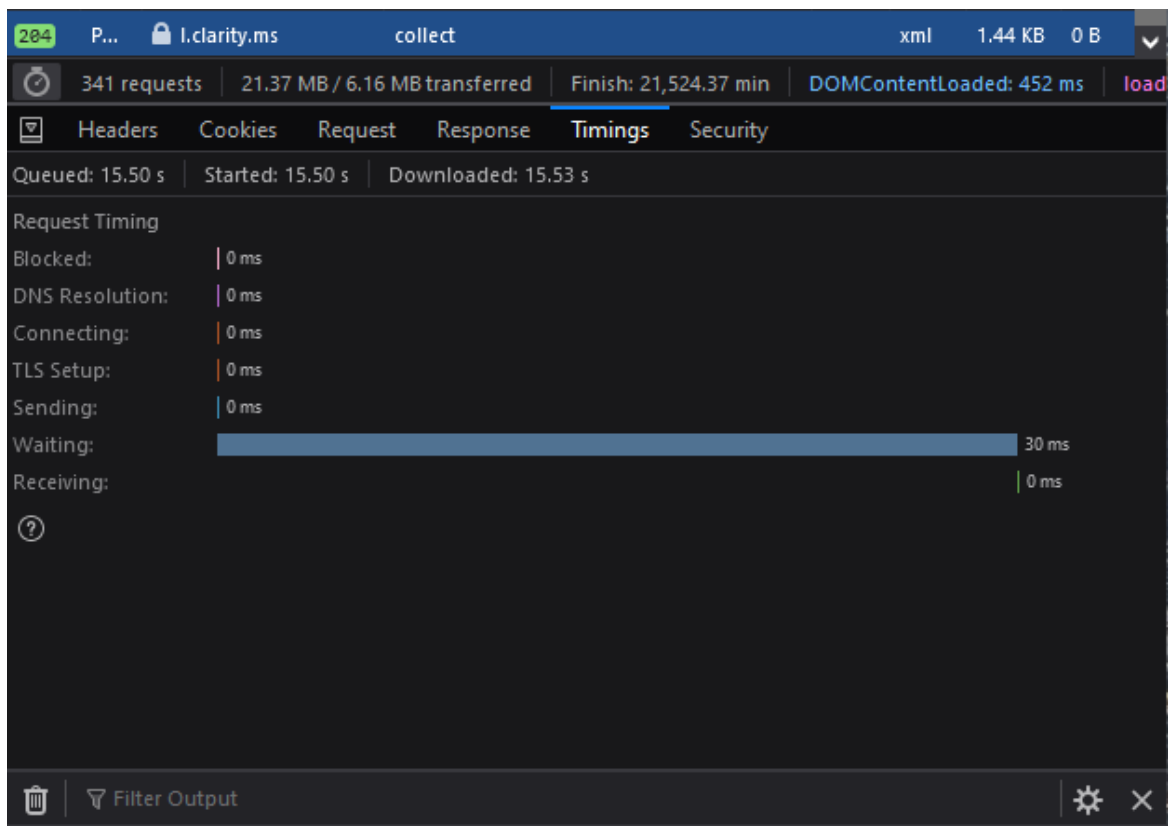
Depicting information sent to one of the Service Replay Providers—Microsoft—through a Service Replay Code—Clarity—after viewing a Studio apartment priced at \$1,488 while visiting www.zillow.com.

50. Similarly, when visiting www.zillow.com, if a user enters personal information in a text box to schedule a tour, that information is captured by the Session Replay Codes embedded on the website:



Depicting information sent to one of the Service Replay Providers—Microsoft—through a Service Replay Code—Clarity—after entering a name (purple text) to a text box to schedule a tour of a property.

51. The eavesdropping by the Session Replay Code is ongoing during the visit and they intercept the contents of these communications between Plaintiff and Zillow with instantaneous transmissions to the Session Replay Providers, as illustrated below, in which only 30 milliseconds were required to send a packet of even response data, which would indicate whatever the website user had just done:



52. The Session Replay Codes operate in the same manner for all putative Class members.

53. Like Plaintiff, each Class member visited www.zillow.com with Session Replay Code embedded in it, and those Session Replay Codes intercepted the Class members' Website Communications with www.zillow.com by sending hyper-frequent logs of those communications to Session Replay Providers.

54. Even if Zillow masks certain elements when it configures the settings of the Session Replay Code embedded on its website, any operational iteration of the Session Replay Code will, by its very nature and purpose, intercept the contents of communications between the website's visitors and the website owner.

55. For example, even with heightened masking enabled, Session Replay Providers will still learn through the intercepted data exactly which pages a user navigates to, how the user moves

through the page (such as which areas the user zooms in on or interacted with), and additional substantive information.

56. As a specific example, if a user types a particular address or zip code into Zillow's main search bar and initiates a search, even if the text entered into the search bar is masked, Session Replay Providers will still learn what is entered into the bar as soon as the search result page loads. This is so because the responsive search results will be displayed on the subsequent page, and the responsive content generated by Zillow will repeat the searched information back on the generated page. That information will not be masked even if user-inputted text is fully masked in a text field.

CLASS ACTION ALLEGATIONS

57. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Class:

All natural persons in the State of Illinois whose Website Communications were captured through the use of Session Replay Code embedded in www.zillow.com.

58. Excluded from the class are Defendant, its parents, subsidiaries, affiliates, officers, and directors, all persons who make a timely election to be excluded from the class, the judge to whom this case is assigned and any immediate family members thereof, and the attorneys who enter their appearance in this action.

59. **Numerosity:** The members of the Class are so numerous that individual joinder of all Class members is impracticable. The precise number of Class members and their identities may be obtained from the books and records of Zillow or the Session Replay Providers.

60. **Commonality:** This action involves questions of law and fact that are common to the Class members. Such common questions include, but are not limited to: (a) whether Defendant employed Session Replay Providers to intercept and record Zillow's website visitors' Website Communications; (b) whether Defendant operated or participated in the operation of an

eavesdropping device; (c) whether Defendant derives a benefit or information from the illegal use of an eavesdropping device; (d) whether Defendant directed another to use an eavesdropping device illegally on its behalf; (e) whether Session Replay Code is an “eavesdropping device” used to intercept or record private electronic communications; (f) whether Defendant acquired the contents of website users’ private electronic communications without their consent; (g) whether Plaintiff and Class members had a reasonable expectation of privacy in their Website communications; (f) whether Defendant violated the Illinois Eavesdropping Act 720 ILCS 5/14-1, *et seq.*; (g) whether Defendant’s interception of Plaintiff’s and Class members’ private electronic communications is an unfair or deceptive act or practice; (h) whether Zillow’s conduct violates the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.* (i) whether Plaintiff and the Class members are entitled to equitable relief; and (j) whether Plaintiff and the Class members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

61. **Typicality:** Plaintiff’s claims are typical of the other Class members’ claims because, among other things, all Class members were comparably injured through the uniform prohibited conduct described above. For instance, Plaintiff and each member of the Class had their electronic communications intercepted in violation of the law and their right to privacy. This uniform injury and the legal theories that underpin recovery make the claims of Plaintiff and the members of the Class typical of one another.

62. **Adequacy of Representation:** Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiff has no interest that is antagonistic to the interests of the Class, and Defendant

has no defenses unique to any Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiff nor his counsel have any interest adverse to the interests of the other members of the Class.

63. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

64. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant intercepted Plaintiff's and Class members' Website Communications, then Plaintiff and each Class member suffered damages by that conduct.

65. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class members may be readily identified through Zillow's books and records or the Session Replay Providers' books and records.

COUNT I
Violation of Illinois Eavesdropping Act
720 ILCS 5/14-1, *et seq.*

66. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

67. Plaintiff brings this claim individually and on behalf of the Class.

68. The Illinois Eavesdropping Act (the “Act”) prohibits (1) using an eavesdropping device in a surreptitious manner to overhear, transmit, or record all or any part of any private conversation; (2) intercepting, recording, or transcribing, in a surreptitious manner, any private electronic communication without consent; (3) manufacturing, assembling, distributing, or possessing any electronic, mechanical, eavesdropping, or other device knowing that or having reason to know that the design of the device renders it primarily useful for the purpose of surreptitious overhearing, transmitting, or recording of private conversations or the intersection; or (4) using or disclosing any information which he or she knows or reasonably should know was obtained from a private conversation or private electronic communication without the consent of all parties to the private electronic communication. 720 ILCS 5/14-2.

69. Any party to any conversation or private electronic communication upon which eavesdropping was practiced shall be entitled to (1) an injunction to prohibit further eavesdropping; (2) actual damages; and (3) punitive damages. punitive damages; 720 ILCS 5/14-6.

70. “Eavesdropping device” is defined as any “any device capable of being used to hear or record oral conversation or intercept, or transcribe electronic communications whether such conversation or electronic communication is conducted in person, by telephone, or by any other means[.]” 720 ILCS 5/14-1(a).

71. “Eavesdropper” is defined as “any person, including any law enforcement officer and any party to a private conversation, who operates or participates in the operation of any eavesdropping device contrary to the provisions of this Article or who acts as a principal, as defined in this Article.” 720 ILCS 5/14-1(b).

72. “Principle” is defined as “any person who: (1) knowingly employs another who illegally uses an eavesdropping device in the course of such employment; or (2) knowingly derives any benefit or information from the illegal use of an eavesdropping device by another; or (3) directs another to use an eavesdropping device illegally on his or her behalf.” 720 ILCS 5/14-1(c).

73. “Private electronic communication” is defined as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation. A reasonable expectation shall include any expectation recognized by law, including, but not limited to, an expectation derived from a privilege, immunity, or right established by common law, Supreme Court rule, or the Illinois or United States Constitution.” ILCS 5/14-1(e).

74. “Surreptitious” is defined as being “obtained or made by stealth or deception, or executed through secrecy or concealment.” 720 ILCS 5/14-1(g).

75. Zillow is an “Eavesdropper” and “Principal” for purposes of the Act because it operates or participates in the operation of an eavesdropping device, knowingly employs another who illegally uses an eavesdropping device, derives a benefit or information from the illegal use of an eavesdropping device, and directs another to use an eavesdropping device illegally on its behalf.

76. Session Replay Code like that operated and employed at Zillow’s direction is a “eavesdropping device” used to transcribe electronic communications within the meaning of the Act.

77. The Session Replay Providers are not a party to the Website Communications—Plaintiff and the Class only knew they were communicating with Zillow, not the Session Replay Providers.

78. Plaintiff's and Class members' intercepted Website Communications constitute the private electronic communications and private conversations within the meaning of the Act.

79. Zillow intentionally operated and employed Session Replay Code on its website to spy on, automatically and secretly, and intercept its website visitors' private electronic interactions communications with Zillow in real time.

80. Plaintiff's and Class members' private electronic communications were intercepted contemporaneously with their transmission.

81. Plaintiff and Class members had a reasonable expectation of privacy in their Website Communications based on the detailed information the Session Replay Code collected from Plaintiff and Class members.

82. Plaintiff and Class members did not consent to having their Website Communications surreptitiously intercepted and recorded.

83. Pursuant to 720 ILCS 5/14-6, Plaintiff and members of the Class are entitled to: (1) an injunction to prohibit further eavesdropping; (2) actual damages; and (3) punitive damages.

84. Zillow's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT II

**Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act
815 ILCS 505/1 *et seq.***

85. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

86. Plaintiff brings this claim individually and on behalf of the Class.

87. The Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.* (“ICFA”) protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

88. The ICFA prohibits “unfair or deceptive acts or practices,” including “misrepresentation or the concealment, suppression or omission of any material fact.” 815 ILCS 505/2.

89. The ICFA applies to Zillow’s conduct described herein because it protects consumers in transactions that are intended to result, or which have resulted in the sale of goods or services.

90. Zillow is a “person” within the meaning of ILCS 505/1(c) because it is a corporation.

91. Plaintiff and members of the Class are “consumers” within the meaning of 815 ILCS 505/1(e) because they visited www.zillow.com to shop for, purchase, or contract to purchase “merchandise”—real estate—for their own use.

92. Zillow’s advertising, offering for sale, and sale of real estate on www.zillow.com is considered “trade” or “commerce” within the meaning of 815 ILCS 505/1(f).

93. Zillow violated the ICFA by concealing material facts about www.zillow.com. Specifically, Zillow omitted and concealed that it directed Session Replay Providers to secretly

monitor, collect, transmit, and discloses its website visitors' Website Communications to the Session Replay Providers using Session Replay Code.

94. Zillow's direction and employment of the Session Replay Providers and their Session Replay Codes to intercept, collect, and disclose website visitors' Website Communications are material to the transactions on www.zillow.com. Zillow is leading online residential real estate marketplace in the United States and Zillow does not disclose its use of Session Replay Code to secretly monitor and collect website visitors' Website Communications. Had Plaintiff and the Class members known that the Session Replay Codes (that collect, transmit, and disclose Website Communications to the Session Replay Providers) were embedded in Zillow's website, they would not have visited www.zillow.com to shop for, purchase, or contract to purchase real estate or they would have required Zillow to compensate them for the interception, collection, and disclosure of their Website Communications.

95. Zillow's intentionally concealed the interception, collection, and disclosure of website visitors' Website Communications using Session Replay Code embedded in www.zillow.com is material because it knows that consumers would not otherwise visit its website to search for, purchase, and contract to purchase real estate. Indeed, Zillow's concealment of such facts was intended to mislead consumers.

96. Zillow's concealment, suppression, and omission of material facts was likely to mislead reasonable consumers under the circumstances, and thus constitutes an unfair and deceptive trade practice in violation of the ICFA.

97. By failing to disclose and inform Plaintiff and the Class about its interception, collection, and disclosure of website visitors' Website Communications, Zillow violated section 505/2 of the ICFA.

98. As a direct and proximate result of these unfair and deceptive practices, Plaintiff and each Class member has suffered actual harm in the form of money and/or property because the disclosure of their Website Communications has value as demonstrated by the collection and use of it by Zillow. The collection and use of this information has now diminished the value of such information to Plaintiff and the Class.

99. As such, Plaintiff and the Class seek an order (1) requiring Zillow to cease the unfair practices described herein; (2) awarding actual damages; and (3) awarding reasonable attorneys' fees and costs.

100. Zillow's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT III
Invasion of Privacy – Intrusion Upon Seclusion

101. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

102. Illinois common law recognizes the tort of invasion of privacy. The right to privacy is also embodied in the Illinois constitution.

103. Plaintiff brings this claim individually and on behalf of the Class.

104. Plaintiff and Class members had an objective, reasonable expectation of privacy in their Website Communications.

105. Plaintiff and Class members did not consent to, authorize, or know about Zillow's intrusion at the time it occurred. Plaintiff and Class members never agreed that Zillow could collect or disclose their Website Communications.

106. Plaintiff and Class members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

107. Zillow intentionally intruded on Plaintiff's and Class members' private life, seclusion, or solitude, without consent.

108. Zillow's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

109. Plaintiff and Class members were harmed by Zillow's wrongful conduct as Zillow's conduct has caused Plaintiff and the Class mental anguish and suffering arising from their loss of privacy and confidentiality of their electronic communications.

110. Zillow's conduct has needlessly harmed Plaintiff and the Class by capturing intimately personal facts and data in the form of their Website Communications. This disclosure and loss of privacy and confidentiality has caused Plaintiff and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

111. Additionally, given the monetary value of individual personal information, Defendant deprived Plaintiff and Class members of the economic value of their interactions with Defendant's website, without providing proper consideration for Plaintiff's and Class members' property.

112. Further, Zillow has improperly profited from its invasion of Plaintiff and Class members' privacy in its use of their data for its economic value.

113. As a direct and proximate result Zillow's conduct, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

114. Zillow's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with session replay software enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

REQUEST FOR RELIEF

Plaintiff, individually and on behalf of the other members of the proposed Class, respectfully requests that the Court enter judgment in Plaintiff's and the Class's favor and against Defendant as follows:

- A. Certifying the Class and appointing Plaintiff as the Class representative;
- B. Appointing Plaintiff's counsel as class counsel;
- C. Declaring that Defendant's past conduct was unlawful, as alleged herein;
- D. Declaring Defendant's ongoing conduct is unlawful, as alleged herein;
- E. Enjoining Defendant from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;
- F. Awarding Plaintiff and the Class members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;
- G. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

H. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

I. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the Class, demands a trial by jury of any and all issues in this action so triable of right.

Dated: September 8, 2022

Respectfully submitted,

/s/ Jonathan M. Jagher

Jonathan M. Jagher

**FREED KANNER LONDON
& MILLEN LLC**

923 Fayette Street

Conshohocken, Pennsylvania 19428

(610) 234-6486

jjagher@fklmlaw.com

Douglas A. Millen

Michael E. Moskovitz

**FREED KANNER LONDON
& MILLEN LLC**

2201 Waukegan Road, Ste. 130

Bannockburn, IL 60015

(224) 632-4500

dmillen@fklmlaw.com

mmoskovitz@fklmlaw.com

Exhibit D

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS**

MARK CONLISK and MICHAEL
DEKHTYAR, individually and on behalf of
all others similarly situated,

Plaintiffs,

v.

ZILLOW GROUP, INC.,

Defendant.

Case No. _____

JURY TRIAL DEMANDED

COMPLAINT - CLASS ACTION

Plaintiffs Mark Conlisk and Michael Dekhtyar (“Plaintiffs”), individually and on behalf of all others similarly situated, hereby file this class action complaint against Defendant Zillow Group, Inc. (“Defendant” or “Zillow”), and in support thereof alleges the following:

INTRODUCTION

1. This is a class action brought against Zillow, the leading online homebuying marketplace, for surreptitiously intercepting the private electronic communications of visitors to its website, www.zillow.com, without their consent.

2. Zillow knowingly directs third-party vendors, such as Microsoft Corporation, to embed snippets of JavaScript computer code (“Session Replay Code”) on Zillow’s website, which then deploys on each website visitor’s internet browser for the purpose intercepting and recording the website visitor’s private electronic communications with the Zillow website, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time (“Website

Communications”). These third-party vendors (collectively, “Session Replay Providers”) create and deploy the Session Replay Code at Zillow’s request.

3. After intercepting and recording the Website Communications, Zillow and the Session Replay Providers use those Website Communications to recreate website visitors’ entire visit to www.zillow.com. The Session Replay Providers create a video replay of the user’s behavior on the website and provide it to Zillow for analysis. Zillow’s directive to the Session Replay Providers to secretly deploy the Session Replay Code results in the electronic equivalent of “looking over the shoulder” of each visitor to the Zillow website for the entire duration of their website interaction.

4. Zillow’s conduct violates the Illinois Eavesdropping Act, 720 ILCS 5/14-1, *et seq.*, the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.*, and constitutes an invasion of the privacy rights of website visitors.

5. Plaintiffs bring this action individually and on behalf of a class of all Illinois citizens whose Website Communications were intercepted at Zillow’s direction and use of Session Replay Code embedded on the webpages of www.zillow.com and seek all civil remedies provided under the causes of action, including but not limited to compensatory, statutory, and/or punitive damages, and attorneys’ fees and costs.

PARTIES

Plaintiff Mark Conlisk

6. Plaintiff Mark Conlisk is a citizen of the state of Illinois, and at all times relevant to this action, resided and was domiciled in Illinois. Plaintiff is a citizen of Illinois.

Plaintiff Michael Dekhtyar

7. Plaintiff Michael Dekhtyar is a citizen of the state of Illinois, and at all times relevant to this action, resided and was domiciled in Illinois. Plaintiff is a citizen of Illinois.

Defendant Zillow Group, Inc.

8. Defendant Zillow Group, Inc. is a corporation organized under the laws of Washington, and its principal place of business is located at 1301 Second Ave., Floor 31, Seattle Washington, 98101. Defendant is a citizen of Washington.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of \$5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class, including the Plaintiffs, who are citizens of a state (Illinois) different than Defendant (Washington).

10. This Court has personal jurisdiction over Defendant because a substantial part of the events and conduct giving rise to Plaintiffs' claims occurred in Illinois. The privacy violations complained of herein resulted from Defendant's purposeful and tortious acts directed towards citizens of Illinois while they were located within Illinois. At all relevant times, Defendant knew that its practices would directly result in collection of information from Illinois citizens while those citizens browse www.zillow.com. Defendant chose to avail itself of the business opportunities of making its real property and rental advertising services specifically available in Illinois (and specifically with respect to Illinois properties) and collecting real-time data from website visit sessions initiated by Illinoisans while located in Illinois, and the claims alleged herein arise from those activities.

11. Zillow also knows that many users visit and interact with Zillow’s websites while they are physically present in Illinois. Both desktop and mobile versions of Zillow’s website allow a user to search for nearby properties by providing the user’s “current location,” as furnished by the location-determining tools of the device the user is using or by the user’s IP address (*i.e.*, without requiring the user to manually input an address). Users’ employment of automatic location services in this way means that Zillow is continuously made aware that its website is being visited by people located in Illinois, and that such website visitors are being eavesdropped on in violation Illinois statutory and common law.

12. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

FACTUAL ALLEGATIONS

A. Website User and Usage Data Have Immense Economic Value.

13. The “world’s most valuable resource is no longer oil, but data.”¹

14. Earlier this year, Business News Daily reported that some businesses collect personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data (*i.e.*, how consumers interact with a business’s website, applications, and emails), behavioral data (*i.e.*, customers’ purchase histories and product usage information), and attitudinal data (*i.e.*, data on consumer satisfaction) from consumers.² This information is valuable to companies because

¹ *The world’s most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

² Max Freedman, *How Businesses Are Collecting Data (And What They’re Doing With It)*, Business News Daily (Aug. 5, 2022), <https://www.businessnewsdaily.com/10625-businesses-collecting-data.html>.

they can use this data to improve customer experiences, refine their marketing strategies, capture data to sell it, and even to secure more sensitive consumer data.³

15. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business's success. Research shows that organizations who "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."⁴

16. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."⁵ In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."⁶

17. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e. \$2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55."⁷

³ *Id.*

⁴ Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), <https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data>.

⁵ Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), <https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf>.

⁶ *Id.* at 25.

⁷ *Id.*

B. Website Users Have a Reasonable Expectation of Privacy in Their Interactions with Websites.

18. Consumers are skeptical and are wary about their data being collected. A report released by KPMG shows that “a full 86% of the respondents said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected.”⁸

19. Another recent paper also indicates that most website visitors will assume their detailed interactions with a website will only be used by the website and not be shared with a party they know nothing about.⁹ As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.¹⁰

20. Privacy polls and studies show that a majority of Americans consider one of the most important privacy rights to be the need for an individual’s affirmative consent before a company collects and shares its customers’ data.

21. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers’ data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.¹¹

⁸ Lance Whitney, *Data privacy is a growing concern for more consumers*, TechRepublic (Aug. 17, 2021), <https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/>.

⁹ *CUJO AI Recent Survey Reveals U.S. Internet Users Expectations and Concerns Towards Privacy and Online Tracking*, CUJO (May 26, 2020), <https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html>.

¹⁰ Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, The Information Society, 38:4, 257, 258 (2022).

¹¹ *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, Consumer Reports (May 11, 2017), <https://www.consumerreports.org/consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/>.

22. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.¹²

23. Users act consistently with their expectation of privacy. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.¹³

C. How Session Replay Code Works.

24. Session Replay Code, such as that implemented on www.zillow.com, enables website operators to record, save, and replay website visitors' interactions with a given website. The clandestinely deployed code provides online marketers and website designers with insights into the user experience by recording website visitors "as they click, scroll, type or navigate across different web pages."¹⁴

25. While Session Replay Code is utilized by websites for some legitimate purposes, it goes well beyond normal website analytics when it comes to collecting the actual contents of communications between website visitors and websites. Unlike other online advertising tools, Session Replay Code allows a website to capture and record nearly every action a website visitor takes while visiting the website, including actions that reveal the visitor's personal or private sensitive data, sometimes even when the visitor does not intend to submit the data to the website

¹² *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, (Nov. 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-Confusedand-feeling-lack-of-control-over-their-personal-information/>.

¹³ Margaret Taylor, *How Apple screwed Facebook*, Wired, (May 19, 2021), <https://www.wired.co.uk/article/apple-ios14-facebook>.

¹⁴ Erin Gilliam Haije, *[Updated] Are Session Recording Tools a Risk to Internet Privacy?*, Mopinion (Mar. 7, 2018), <https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/>.

operator, or has not finished submitting the data to the website operator.¹⁵ As a result, website visitors “aren’t just sharing data with the [web]site they’re on . . . but also with an analytics service that may be watching over their shoulder.”¹⁶

26. Session Replay Code works by inserting computer code into the various event handling routines that web browsers use to receive input from users, thus intercepting the occurrence of actions the user takes. When a website delivers Session Replay Code to a user’s browser, the browser will follow the code’s instructions by sending responses in the form of “event” data to a designated third-party server. Typically, the server receiving the event data is controlled by the third-party entity that wrote the Session Replay Code, rather than the owner of the website where the code is installed.

27. The types of events captured by Session Replay Code vary by specific product and configuration, but in general are wide-ranging and can encompass virtually every user action, including all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entry, and numerous other forms of a user’s navigation and interaction through the website. In order to permit a reconstruction of a user’s visit accurately, the Session Replay Code must be capable of capturing these events at hyper-frequent intervals, often just milliseconds apart. Events are typically accumulated and transmitted in blocks periodically throughout the user’s website session, rather than after the user’s visit to the website is completely finished.

28. Unless specifically masked through configurations chosen by the website owner, some visible contents of the website may also be transmitted to the Session Replay Provider.

¹⁵ *Id.*

¹⁶ Eric Ravenscraft, *Almost Every Website You Visit Records Exactly How Your Mouse Moves*, Medium (Feb. 5, 2020), <https://onezero.medium.com/almost-every-website-you-visit-records-exactly-how-your-mouse-moves-4134cb1cc7a0>.

29. Once the events from a user session have been recorded by a Session Replay Code, a website operator can view a visual reenactment of the user's visit through the Session Replay Provider, usually in the form of a video, meaning "[u]nlike typical analytics services that provide aggregate statistics, these scripts are intended for the recording and playback of individual browsing sessions."¹⁷

30. Because most Session Replay Codes will by default indiscriminately capture the maximum range of user-initiated events and content displayed by the website, researchers have found that a variety of highly sensitive information can be captured in event responses from website visitors, including medical conditions, credit card details, and other personal information displayed or entered on webpages.¹⁸

31. Most alarming, Session Replay Code may capture data that the user did not even intentionally transmit to a website during a visit, and then make that data available to website owners when they access the session replay through the Session Replay Provider. For example, if a user writes information into a text form field, but then chooses not to click a "submit" or "enter" button on the website, the Session Replay Code may nevertheless cause the non-submitted text to be sent to the designated event-response-receiving server before the user deletes the text or leaves the page. This information will then be viewable to the website owner when accessing the session replay through the Session Replay Provider.

32. Session Replay Code does not necessarily anonymize user sessions, either.

¹⁷ Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), <https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/>.

¹⁸ *Id.*

33. First, if a user’s entry of personally identifying information is captured in an event response, that data will become known and visible to both the Session Replay Provider and the website owner.

34. Second, if a website displays user account information to a logged-in user, that content may be captured by Session Replay Code.

35. Third, some Session Replay Providers explicitly offer website owners cookie functionality that permits linking a session to an identified user, who may be personally identified if the website owner has associated the user with an email address or username.¹⁹

36. Session Replay Providers often create “fingerprints” that are unique to a particular user’s combination of computer and browser settings, screen configuration, and other detectable information. The resulting fingerprint, which is often unique to a user and rarely changes, are collected across all sites that the Session Replay Provider monitors.

37. When a user eventually identifies themselves to one of these websites (such as by filling in a form), the provider can then associate the fingerprint with the user identity and can then back-reference all of that user’s other web browsing across other websites previously visited, including on websites where the user had intended to remain anonymous—even if the user explicitly indicated that they would like to remain anonymous by enabling private browsing.

38. In addition to the privacy invasions caused by the diversion of user communications with websites to third-party Session Replay Providers, Session Replay Code also exposes website visitors to identity theft, online scams, and other privacy threats.²⁰ Indeed, “[t]he more copies of

¹⁹ *Id.*; see also *FS.identify – Identifying users*, FullStory, <https://help.fullstory.com/hc/en-us/articles/360020828113>, (last visited Sep. 8, 2022).

²⁰ Juha Sarrinen, *Session Replay is a Major Threat to Privacy on the Web*, itnews (Nov. 16, 2017), <https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720>.

sensitive information that exist, the broader the attack surface, and when data is being collected [] it may not be stored properly or have standard protections” increasing “the overall risk that data will someday publicly leak or be breached.”²¹

39. Recognizing the privacy concerns posed by Session Replay Code, in 2019 Apple required app developers to remove or properly disclose the use of analytics code that allow app developers to record how a user interacts with their iPhone apps or face immediate removal from the app store.²² In announcing this decision, Apple stated: “Protecting user privacy is paramount in the Apple ecosystem. Our App Store Review Guidelines require that apps request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity.”²³

D. Zillow Secretly Eavesdrops on its Website Visitors’ Electronic Communications.

40. Zillow operates the website www.zillow.com. Zillow is the “leading online residential real estate” marketplace in the United States for consumers, connecting them to the information and real estate professionals they need to buy, sell, or rent a home.²⁴

41. Zillow has become “synonymous with residential real estate.”²⁵ www.zillow.com is the most popular real estate website in the United States, with over thirty-six million unique

²¹ Lily Hay Newman, *Covert ‘Replay Sessions’ Have Been harvesting Passwords by Mistake*, WIRED (Feb. 26, 2018), <https://www.wired.com/story/covert-replay-sessions-harvesting-passwords/>.

²² Zack Whittaker, *Apple Tells App Developers to Disclose or Remove Screen Recording Code*, TechCrunch (Feb. 7, 2019), <https://techcrunch.com/2019/02/07/apple-glassbox-apps/>.

²³ *Id.*

²⁴ Zillow Group, Inc., *Form 10-K* (Dec. 31, 2021), <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001617640/87bbb30-39cb-4eb7-acdc-1b51265b9687.pdf> (“Zillow 10-K”).

²⁵ *Id.*

monthly visitors²⁶ and more than 135 million properties are listed on its website.²⁷ According to a 2021 Google Trends report, “[t]oday more people search ‘Zillow’ than ‘real estate.’”²⁸

42. However, unbeknownst to the millions of individuals perusing Zillow’s real estate listings, Zillow knowingly directs Session Replay Providers to embed various Session Replay Codes on its website to track and analyze website user interactions with www.zillow.com. Because the Session Replay Providers are unknown eavesdroppers to visitors to www.zillow.com, they are not parties to website visitors’ Website Communications with Zillow.

43. One such Session Replay Provider that Zillow procures is Microsoft.

44. Microsoft is the owner and operator of a Session Replay Code titled Clarity, which provides basic information about website user sessions, interactions, and engagement, and breaks down users by device type, county, and other dimensions.²⁹

45. Zillow knowingly derives a benefit and/or information from the Website Communications intercepted and recorded at its direction. Upon information and belief, Zillow uses the intercepted Website Communications to replay website visitors’ interactions with www.zillow.com, improve user interactions with its website, and to provide targeted real estate advertisements to its website visitors.

46. Zillow’s knowing direction and use of Microsoft Clarity’s Session Replay Code, direction and use of other Session Replay Codes through various Session Replay Providers, and its knowing derivation of a benefit and/or information from the Website Communications

²⁶ *Most Popular Real Estate Websites in the United States as of October 2021, Based on Unique Monthly Visits*, Statista, <https://www.statista.com/statistics/381468/most-popular-real-estate-websites-by-monthly-visits-usa/>, (last visited Sep. 8, 2022).

²⁷ Zillow 10-K, *supra*, note 1.

²⁸ *Id.*

²⁹ Jono Alderson, *An Introduction to Microsoft Clarity*, Yoast, <https://yoast.com/introduction-microsoft-clarity/#h-what-is-microsoft-clarity>, (last visited Sep. 8, 2022).

surreptitiously intercepted and recorded by Session Replay Codes is a violation of Illinois statutory and common law.

E. Plaintiffs' and Class Members' Experiences.

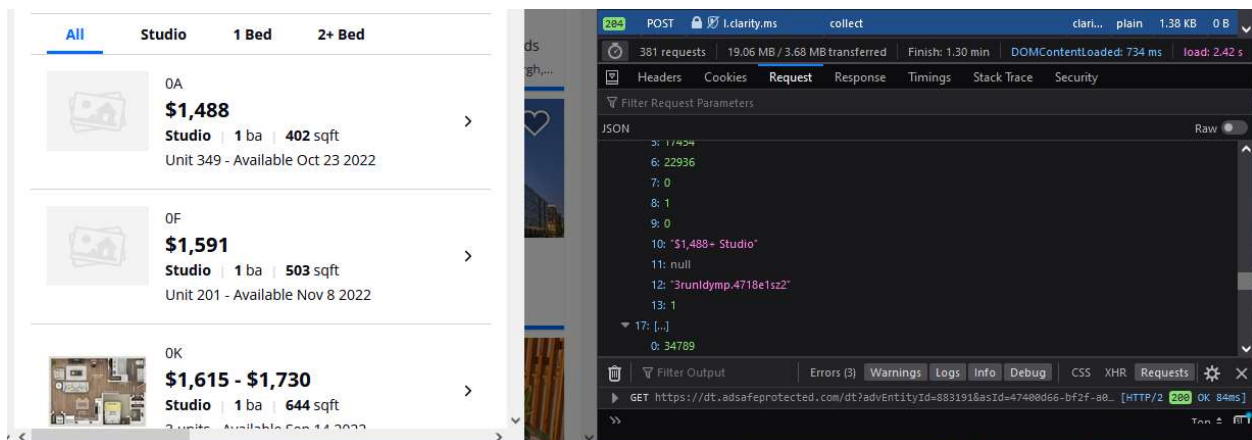
47. Plaintiffs have each independently visited www.zillow.com on his device while in Illinois on at least one occasion.

48. While visiting Zillow's website, Plaintiffs fell victim to Defendant's unlawful monitoring, recording, and collection of Plaintiffs' Website Communications with www.zillow.com.

49. Unknown to Plaintiffs, Zillow directs Session Replay Providers to embed Session Replay Code on its website.

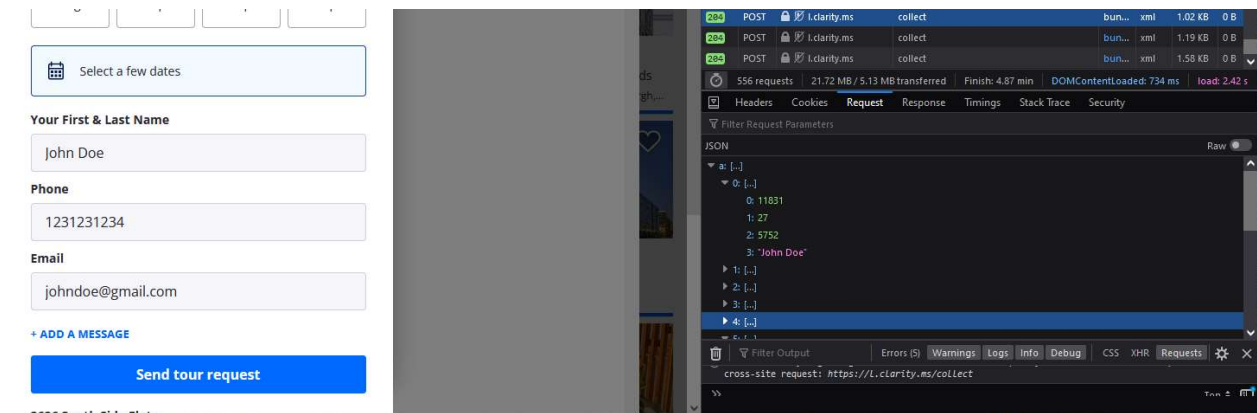
50. During the website visit(s), Plaintiffs' Website Communications were captured by Session Replay Code and sent to various Session Replay Providers.

51. For example, when visiting www.zillow.com, if a website user views a certain piece of property for rent or sale, that information is captured by the Session Replay Codes embedded on the website:



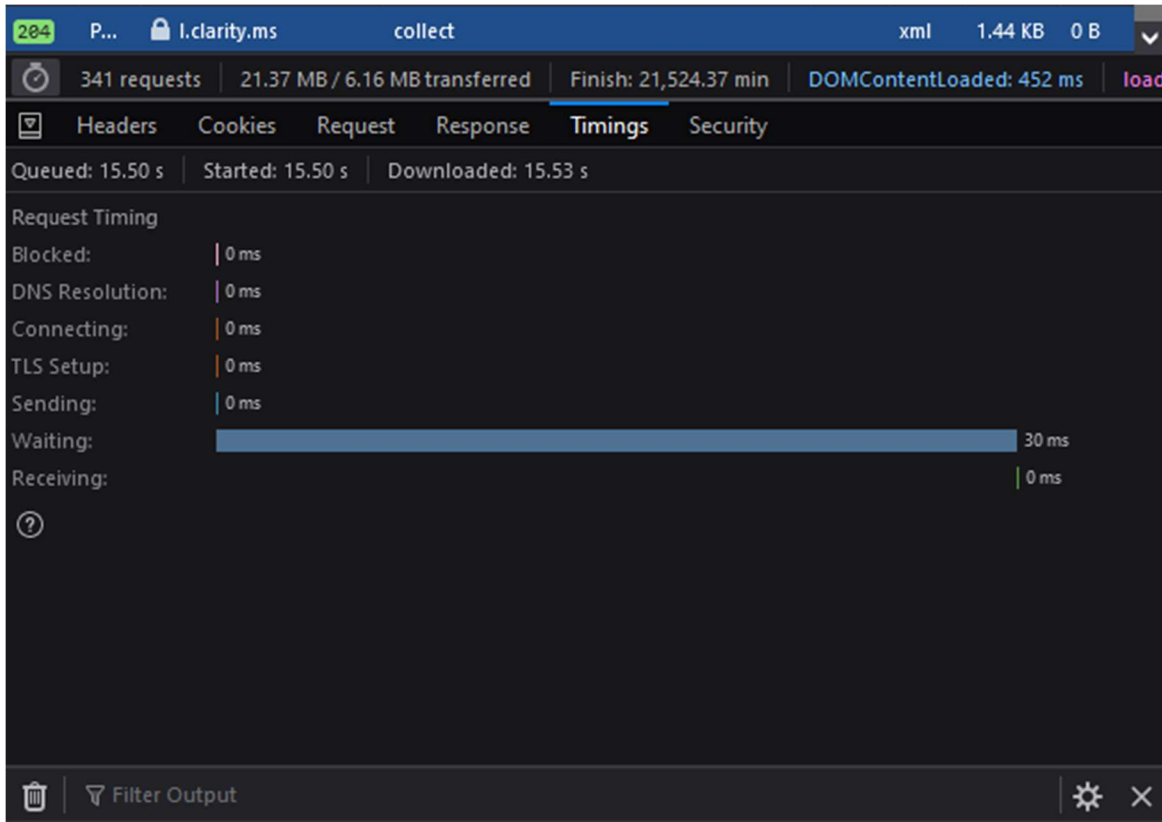
Depicting information sent to one of the Service Replay Providers—Microsoft—through a Service Replay Code—Clarity—after viewing a Studio apartment priced at \$1,488 while visiting www.zillow.com.

52. Similarly, when visiting www.zillow.com, if a user enters personal information in a text box to schedule a tour, that information is captured by the Session Replay Codes embedded on the website:



Depicting information sent to one of the Service Replay Providers—Microsoft—through a Service Replay Code—Clarity—after entering a name (purple text) to a text box to schedule a tour of a property.

53. The eavesdropping by the Session Replay Code is ongoing during the visit and they intercept the contents of these communications between Plaintiffs and Zillow with instantaneous transmissions to the Session Replay Providers, as illustrated below, in which only 30 milliseconds were required to send a packet of even response data, which would indicate whatever the website user had just done:



54. The Session Replay Codes operate in the same manner for all putative Class members.

55. Like Plaintiffs, each Class member visited www.zillow.com with Session Replay Code embedded in it, and those Session Replay Codes intercepted the Class members' Website Communications with www.zillow.com by sending hyper-frequent logs of those communications to Session Replay Providers.

56. Even if Zillow masks certain elements when it configures the settings of the Session Replay Code embedded on its website, any operational iteration of the Session Replay Code will, by its very nature and purpose, intercept the contents of communications between the website's visitors and the website owner.

57. For example, even with heightened masking enabled, Session Replay Providers will still learn through the intercepted data exactly which pages a user navigates to, how the user moves

eavesdropping device; (c) whether Defendant derives a benefit or information from the illegal use of an eavesdropping device; (d) whether Defendant directed another to use an eavesdropping device illegally on its behalf; (e) whether Session Replay Code is an “eavesdropping device” used to intercept or record private electronic communications; (f) whether Defendant acquired the contents of website users’ private electronic communications without their consent; (g) whether Plaintiffs and Class members had a reasonable expectation of privacy in their Website communications; (f) whether Defendant violated the Illinois Eavesdropping Act 720 ILCS 5/14-1, *et seq.*; (g) whether Defendant’s interception of Plaintiffs’ and Class members’ private electronic communications is an unfair or deceptive act or practice; (h) whether Zillow’s conduct violates the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.* (i) whether Plaintiffs and the Class members are entitled to equitable relief; and (j) whether Plaintiffs and the Class members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

63. **Typicality:** Plaintiffs’ claims are typical of the other Class members’ claims because, among other things, all Class members were comparably injured through the uniform prohibited conduct described above. For instance, Plaintiffs and each member of the Class had their electronic communications intercepted in violation of the law and their right to privacy. This uniform injury and the legal theories that underpin recovery make the claims of Plaintiffs and the members of the Class typical of one another.

64. **Adequacy of Representation:** Plaintiffs have and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiffs have retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiffs have no interest that is antagonistic to the interests of the Class, and

Defendant has no defenses unique to any Plaintiff(s). Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to the interests of the other members of the Class.

65. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

66. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiffs and each member of the Class. If Defendant intercepted Plaintiffs' and Class members' Website Communications, then Plaintiffs and each Class member suffered damages by that conduct.

67. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class members may be readily identified through Zillow's books and records or the Session Replay Providers' books and records.

COUNT I
Violation of Illinois Eavesdropping Act
720 ILCS 5/14-1, *et seq.*

68. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

69. Plaintiffs bring this claim individually and on behalf of the Class.

70. The Illinois Eavesdropping Act (the “Act”) prohibits (1) using an eavesdropping device in a surreptitious manner to overhear, transmit, or record all or any part of any private conversation; (2) intercepting, recording, or transcribing, in a surreptitious manner, any private electronic communication without consent; (3) manufacturing, assembling, distributing, or possessing any electronic, mechanical, eavesdropping, or other device knowing that or having reason to know that the design of the device renders it primarily useful for the purpose of surreptitious overhearing, transmitting, or recording of private conversations or the intersection; or (4) using or disclosing any information which he or she knows or reasonably should know was obtained from a private conversation or private electronic communication without the consent of all parties to the private electronic communication. 720 ILCS 5/14-2.

71. Any party to any conversation or private electronic communication upon which eavesdropping was practiced shall be entitled to (1) an injunction to prohibit further eavesdropping; (2) actual damages; and (3) punitive damages. punitive damages; 720 ILCS 5/14-6.

72. “Eavesdropping device” is defined as any “any device capable of being used to hear or record oral conversation or intercept, or transcribe electronic communications whether such conversation or electronic communication is conducted in person, by telephone, or by any other means[.]” 720 ILCS 5/14-1(a).

73. “Eavesdropper” is defined as “any person, including any law enforcement officer and any party to a private conversation, who operates or participates in the operation of any eavesdropping device contrary to the provisions of this Article or who acts as a principal, as defined in this Article.” 720 ILCS 5/14-1(b).

74. “Principle” is defined as “any person who: (1) knowingly employs another who illegally uses an eavesdropping device in the course of such employment; or (2) knowingly derives any benefit or information from the illegal use of an eavesdropping device by another; or (3) directs another to use an eavesdropping device illegally on his or her behalf.” 720 ILCS 5/14-1(c).

75. “Private electronic communication” is defined as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation. A reasonable expectation shall include any expectation recognized by law, including, but not limited to, an expectation derived from a privilege, immunity, or right established by common law, Supreme Court rule, or the Illinois or United States Constitution.” ILCS 5/14-1(e).

76. “Surreptitious” is defined as being “obtained or made by stealth or deception, or executed through secrecy or concealment.” 720 ILCS 5/14-1(g).

77. Zillow is an “Eavesdropper” and “Principal” for purposes of the Act because it operates or participates in the operation of an eavesdropping device, knowingly employs another who illegally uses an eavesdropping device, derives a benefit or information from the illegal use of an eavesdropping device, and directs another to use an eavesdropping device illegally on its behalf.

78. Session Replay Code like that operated and employed at Zillow’s direction is a “eavesdropping device” used to transcribe electronic communications within the meaning of the Act.

79. The Session Replay Providers are not a party to the Website Communications—Plaintiffs and the Class only knew they were communicating with Zillow, not the Session Replay Providers.

80. Plaintiffs’ and Class members’ intercepted Website Communications constitute the private electronic communications and private conversations within the meaning of the Act.

81. Zillow intentionally operated and employed Session Replay Code on its website to spy on, automatically and secretly, and intercept its website visitors’ private electronic interactions communications with Zillow in real time.

82. Plaintiffs’ and Class members’ private electronic communications were intercepted contemporaneously with their transmission.

83. Plaintiffs and Class members had a reasonable expectation of privacy in their Website Communications based on the detailed information the Session Replay Code collected from Plaintiffs and Class members.

84. Plaintiffs and Class members did not consent to having their Website Communications surreptitiously intercepted and recorded.

85. Pursuant to 720 ILCS 5/14-6, Plaintiff and members of the Class are entitled to: (1) an injunction to prohibit further eavesdropping; (2) actual damages; and (3) punitive damages.

86. Zillow’s conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiffs and Class members any time they visit Defendant’s website with Session Replay Code enabled without their consent. Plaintiffs and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT II

**Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act
815 ILCS 505/1 *et seq.***

87. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

88. Plaintiffs bring this claim individually and on behalf of the Class.

89. The Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.* (“ICFA”) protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

90. The ICFA prohibits “unfair or deceptive acts or practices,” including “misrepresentation or the concealment, suppression or omission of any material fact.” 815 ILCS 505/2.

91. The ICFA applies to Zillow’s conduct described herein because it protects consumers in transactions that are intended to result, or which have resulted in the sale of goods or services.

92. Zillow is a “person” within the meaning of ILCS 505/1(c) because it is a corporation.

93. Plaintiffs and members of the Class are “consumers” within the meaning of 815 ILCS 505/1(e) because they visited www.zillow.com to shop for, purchase, or contract to purchase “merchandise”—real estate—for their own use.

94. Zillow’s advertising, offering for sale, and sale of real estate on www.zillow.com is considered “trade” or “commerce” within the meaning of 815 ILCS 505/1(f).

95. Zillow violated the ICFA by concealing material facts about www.zillow.com. Specifically, Zillow omitted and concealed that it directed Session Replay Providers to secretly

monitor, collect, transmit, and discloses its website visitors' Website Communications to the Session Replay Providers using Session Replay Code.

96. Zillow's direction and employment of the Session Replay Providers and their Session Replay Codes to intercept, collect, and disclose website visitors' Website Communications are material to the transactions on www.zillow.com. Zillow is leading online residential real estate marketplace in the United States and Zillow does not disclose its use of Session Replay Code to secretly monitor and collect website visitors' Website Communications. Had Plaintiffs and the Class members known that the Session Replay Codes (that collect, transmit, and disclose Website Communications to the Session Replay Providers) were embedded in Zillow's website, they would not have visited www.zillow.com to shop for, purchase, or contract to purchase real estate or they would have required Zillow to compensate them for the interception, collection, and disclosure of their Website Communications.

97. Zillow's intentionally concealed the interception, collection, and disclosure of website visitors' Website Communications using Session Replay Code embedded in www.zillow.com is material because it knows that consumers would not otherwise visit its website to search for, purchase, and contract to purchase real estate. Indeed, Zillow's concealment of such facts was intended to mislead consumers.

98. Zillow's concealment, suppression, and omission of material facts was likely to mislead reasonable consumers under the circumstances, and thus constitutes an unfair and deceptive trade practice in violation of the ICFA.

99. By failing to disclose and inform Plaintiffs and the Class about its interception, collection, and disclosure of website visitors' Website Communications, Zillow violated section 505/2 of the ICFA.

100. As a direct and proximate result of these unfair and deceptive practices, Plaintiffs and each Class member has suffered actual harm in the form of money and/or property because the disclosure of their Website Communications has value as demonstrated by the collection and use of it by Zillow. The collection and use of this information has now diminished the value of such information to Plaintiffs and the Class.

101. As such, Plaintiffs and the Class seek an order (1) requiring Zillow to cease the unfair practices described herein; (2) awarding actual damages; and (3) awarding reasonable attorneys' fees and costs.

102. Zillow's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiffs and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT III **Invasion of Privacy – Intrusion Upon Seclusion**

103. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

104. Plaintiffs bring this claim individually and on behalf of the Class.

105. Illinois common law recognizes the tort of invasion of privacy. The right to privacy is also embodied in the Illinois constitution.

106. Plaintiffs and Class members had an objective, reasonable expectation of privacy in their Website Communications.

107. Plaintiffs and Class members did not consent to, authorize, or know about Zillow's intrusion at the time it occurred. Plaintiffs and Class members never agreed that Zillow could collect or disclose their Website Communications.

108. Plaintiffs and Class members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

109. Zillow intentionally intruded on Plaintiffs' and Class members' private life, seclusion, or solitude, without consent.

110. Zillow's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

111. Plaintiffs and Class members were harmed by Zillow's wrongful conduct as Zillow's conduct has caused Plaintiffs and the Class mental anguish and suffering arising from their loss of privacy and confidentiality of their electronic communications.

112. Zillow's conduct has needlessly harmed Plaintiffs and the Class by capturing intimately personal facts and data in the form of their Website Communications. This disclosure and loss of privacy and confidentiality has caused Plaintiffs and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

113. Additionally, given the monetary value of individual personal information, Defendant deprived Plaintiffs and Class members of the economic value of their interactions with Defendant's website, without providing proper consideration for Plaintiffs' and Class members' property.

114. Further, Zillow has improperly profited from its invasion of Plaintiffs and Class members' privacy in its use of their data for its economic value.

115. As a direct and proximate result Zillow's conduct, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

116. Zillow's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiffs and Class members any time they visit Defendant's website with session replay software enabled without their consent. Plaintiffs and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

REQUEST FOR RELIEF

Plaintiffs, individually and on behalf of the other members of the proposed Class, respectfully requests that the Court enter judgment in Plaintiffs' and the Class's favor and against Defendant as follows:

- A. Certifying the Class and appointing Plaintiffs as the Class representatives;
- B. Appointing Plaintiffs' counsel as class counsel;
- C. Declaring that Defendant's past conduct was unlawful, as alleged herein;
- D. Declaring Defendant's ongoing conduct is unlawful, as alleged herein;
- E. Enjoining Defendant from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;
- F. Awarding Plaintiffs and the Class members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;
- G. Awarding Plaintiffs and the Class members pre-judgment and post-judgment interest;

H. Awarding Plaintiffs and the Class members reasonable attorneys' fees, costs, and expenses; and

I. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the Class, demands a trial by jury of any and all issues in this action so triable of right.

DATED: September 19, 2022

Respectfully Submitted,

s/ Gary M. Klinger

Gary M. Klinger

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC

227 W. Monroe Street, Suite 2100

Chicago, IL 60606

Phone: 866.252.0878

gklinger@milberg.com

Nick Suciu III

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC

6905 Telegraph Road, Suite 115

Bloomfield Hills, MI 48301

Tel: (313) 303-3472

nsuciu@milberg.com

[Query](#) [Reports](#) [Utilities](#) [Help](#) [Log Out](#)

GILBERT

United States District Court
Northern District of Illinois - CM/ECF NextGen 1.6.3 (Chicago)
CIVIL DOCKET FOR CASE #: 1:22-cv-05644

Strelzin v. Zillow Group, Inc.
Assigned to: Honorable Steven C. Seeger
Case in other court: Circuit Court of Cook County, Illinois,
2022CH09132
Cause: 28:1332 Diversity-Personal Injury

Date Filed: 10/14/2022
Jury Demand: Plaintiff
Nature of Suit: 360 P.I.: Other
Jurisdiction: Diversity

Plaintiff

Jill Strelzin
*individually and on behalf of all other
similarly situated*

represented by **Katrina Carroll**
Lynch Carpenter LLP
111 West Washington Street
Suite 1240
Chicago, IL 60602
(312) 750-1265
Fax: Not a member
Email: katrina@lcllp.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

V.

Defendant

Zillow Group, Inc.

represented by **David T Cellitti**
Buchanan Ingersoll & Rooney PC
401 E. Jackson Street, Suite 2400
Tempe, FL 33602-5236
(813) 222-1137
Fax: Not a member
Email: david.cellitti@bipc.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
10/14/2022	1	NOTICE of Removal from Circuit Court of Cook County, Illinois, case number (2022CH09132) filed by Zillow Group, Inc. Filing fee \$ 402, receipt number AILNDC-19946139. (Attachments: # 1 Exhibits A through D)(Cellitti, David) (Entered: 10/14/2022)
10/14/2022	2	CIVIL Cover Sheet (Cellitti, David) (Entered: 10/14/2022)
10/14/2022	3	ATTORNEY Appearance for Defendant Zillow Group, Inc. by David T Cellitti (Cellitti, David) (Entered: 10/14/2022)
10/14/2022		CASE ASSIGNED to the Honorable Steven C. Seeger. Designated as Magistrate Judge the

		Honorable Jeffrey T. Gilbert. Case assignment: Random assignment. (emc,) (Entered: 10/14/2022)
10/14/2022	4	NOTIFICATION of Affiliates pursuant to Local Rule 3.2 by Zillow Group, Inc. (Cellitti, David) (Entered: 10/14/2022)
10/17/2022	5	MINUTE entry before the Honorable Steven C. Seeger: An initial status report is due by January 2, 2023. Counsel must read the Standing Order entitled "Initial Status Conferences and Joint Initial Status Reports" on the Court's website. The parties must confer as required by Rule 26(f) about the nature, scope, and duration of discovery. The parties must submit two documents to the Court. First, the parties must file the Joint Initial Status Report under Rule 26(f) on the docket. A Word version of the Joint Initial Status Report is available on the Court's website. All parties must participate in the preparation and filing of the Joint Initial Status Report. The Court requires a joint report, so a filing by one side or the other is not sufficient. Second, the parties must email a Word version of a proposed Scheduling Order under Rule 16(b) to the Court's proposed order inbox. Lead counsel for the parties must participate in filing the initial status report. Plaintiff must serve this Order on all other parties. If the defendant has not been served with process, plaintiff's counsel must contact the Courtroom Deputy at jessica_j_ramos@ilnd.uscourts.gov to reschedule the initial status report deadline. Plaintiff should not file the Joint Initial Status Report before the defendant(s) has been served with process. The parties must discuss settlement in good faith and make a serious attempt to resolve this case amicably. All counsel of record must read and comply with this Court's Standing Orders on its webpage. Please pay special attention to the Standing Orders about Depositions and Discovery. Mailed notice. (jjr,) (Entered: 10/17/2022)
10/17/2022	6	MAILED Notice of Removal letter to counsel of record. (jn,) (Entered: 10/17/2022)
10/17/2022		CLERK'S NOTICE: Pursuant to Local Rule 73.1(b), a United States Magistrate Judge of this court is available to conduct all proceedings in this civil action. If all parties consent to have the currently assigned United States Magistrate Judge conduct all proceedings in this case, including trial, the entry of final judgment, and all post-trial proceedings, all parties must sign their names on the attached Consent To form. This consent form is eligible for filing only if executed by all parties. The parties can also express their consent to jurisdiction by a magistrate judge in any joint filing, including the Joint Initial Status Report or proposed Case Management Order. (jn,) (Entered: 10/17/2022)

PACER Service Center			
Transaction Receipt			
10/19/2022 12:44:04			
PACER Login:	samanthasouthall	Client Code:	0106198-000001-SS
Description:	Docket Report	Search Criteria:	1:22-cv-05644
Billable Pages:	2	Cost:	0.20

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA**

ASHLEY POPA, individually and on behalf
of all others similarly situated,

Plaintiff,

v.

ZILLOW GROUP, INC.,

Defendant.

Case No. 2:22-CV-1287

JURY TRIAL DEMANDED

COMPLAINT - CLASS ACTION

Plaintiff Ashley Popa (“Plaintiff”), individually and on behalf of all others similarly situated, hereby files this class action complaint against Defendant Zillow Group, Inc. (“Defendant” or “Zillow”), and in support thereof alleges the following:

INTRODUCTION

1. This is a class action brought against Zillow for wiretapping the electronic communications of visitors to its website, www.zillow.com. Zillow procures third-party vendors, such as Microsoft Corporation, to embed snippets of JavaScript computer code (“Session Replay Code”) on Zillow’s website, which then deploys on each website visitor’s internet browser for the purpose intercepting and recording the website visitor’s electronic communications with the Zillow website, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time (“Website Communications”). These third-party vendors (collectively, “Session Replay Providers”) create and deploy the Session Replay Code at Zillow’s request.

2. After intercepting and capturing the Website Communications, Zillow and the Session Replay Providers use those Website Communications to recreate website visitors' entire visit to www.zillow.com. The Session Replay Providers create a video replay of the user's behavior on the website and provide it to Zillow for analysis. Zillow's procurement of the Session Replay Providers to secretly deploy the Session Replay Code results in the electronic equivalent of "looking over the shoulder" of each visitor to the Zillow website for the entire duration of their website interaction.

3. Zillow's conduct violates the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Cons. Stat. § 5701, *et. seq.*, and constitutes an invasion of the privacy rights of website visitors.

4. Plaintiff brings this action individually and on behalf of a class of all Pennsylvania citizens whose Website Communications were intercepted through Zillow's procurement and use of Session Replay Code embedded on the webpages of www.zillow.com and seeks all civil remedies provided under the causes of action, including but not limited to compensatory, statutory, and/or punitive damages, and attorneys' fees and costs.

PARTIES

5. Plaintiff Ashley Popa is a citizen of the Commonwealth of Pennsylvania, and at all times relevant to this action, resided and was domiciled in Lawrence County, Pennsylvania. Plaintiff is a citizen of Pennsylvania.

6. Defendant Zillow Group, Inc. is corporation organized under the laws of Washington, and its principal place of business is located at 1301 Second Ave., Floor 31, Seattle Washington, 98101. Defendant is a citizen of Washington.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of \$5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class, including Plaintiff, is a citizen of a state different than Defendant.

8. This Court has personal jurisdiction over Defendant because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in Pennsylvania. The privacy violations complained of herein resulted from Defendant's purposeful and tortious acts directed towards citizens of Pennsylvania while they were located within Pennsylvania. At all relevant times, Defendant knew that its practices would directly result in collection of information from Pennsylvania citizens while those citizens browse www.zillow.com. Defendant chose to avail itself of the business opportunities of making its real property and rental advertising services specifically available in Pennsylvania (and specifically with respect to Pennsylvania properties) and collecting real-time data from website visit sessions initiated by Pennsylvanians while located in Pennsylvania, and the claims alleged herein arise from those activities.

9. Zillow also knows that many users visit and interact with Zillow's websites while they are physically present in Pennsylvania. Both desktop and mobile versions of Zillow's website allow a user to search for nearby properties by providing the user's "current location," as furnished by the location-determining tools of the device the user is using or by the user's IP address (*i.e.*, without requiring the user to manually input an address). Users' employment of automatic location services in this way means that Zillow is continuously made aware that its website is being visited

by people located in Pennsylvania, and that such website visitors are being wiretapped in violation of Pennsylvania statutory and common law.

10. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

FACTUAL ALLEGATIONS

A. Website User and Usage Data Have Immense Economic Value.

11. The “world’s most valuable resource is no longer oil, but data.”¹

12. Earlier this year, Business News Daily reported that some businesses collect personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data (*i.e.*, how consumers interact with a business’s website, applications, and emails), behavioral data (*i.e.*, customers’ purchase histories and product usage information), and attitudinal data (*i.e.*, data on consumer satisfaction) from consumers.² This information is valuable to companies because they can use this data to improve customer experiences, refine their marketing strategies, capture data to sell it, and even to secure more sensitive consumer data.³

13. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business’s success.

¹ *The world’s most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

² Max Freedman, *How Businesses Are Collecting Data (And What They’re Doing With It)*, Business News Daily (Aug. 5, 2022), <https://www.businessnewsdaily.com/10625-businesses-collecting-data.html>.

³ *Id.*

Research shows that organizations who “leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin.”⁴

14. In 2013, the Organization for Economic Cooperation and Development (“OECD”) even published a paper entitled “Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value.”⁵ In this paper, the OECD measured prices demanded by companies concerning user data derived from “various online data warehouses.”⁶

15. OECD indicated that “[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e. \$2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver’s license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55.”⁷

B. Website Users Have a Reasonable Expectation of Privacy in Their Interactions with Websites.

16. Consumers are skeptical and are wary about their data being collected. A report released by KPMG shows that “a full 86% of the respondents said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected.”⁸

⁴ Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), <https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data>.

⁵ Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), <https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf>.

⁶ *Id.* at 25.

⁷ *Id.*

⁸ Lance Whitney, *Data privacy is a growing concern for more consumers*, TechRepublic (Aug. 17, 2021), <https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/>.

17. Another recent paper also indicates that most website visitors will assume their detailed interactions with a website will only be used by the website and not be shared with a party they know nothing about.⁹ As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.¹⁰

18. Privacy polls and studies show that a majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

19. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.¹¹

20. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.¹²

21. Users act consistently with their expectation of privacy. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing

⁹ *CUJO AI Recent Survey Reveals U.S. Internet Users Expectations and Concerns Towards Privacy and Online Tracking*, CUJO (May 26, 2020), <https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html>.

¹⁰ Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, *The Information Society*, 38:4, 257, 258 (2022).

¹¹ *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, Consumer Reports (May 11, 2017), <https://www.consumerreports.org/consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/>.

¹² *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, (Nov. 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-Confusedand-feeling-lack-of-control-over-their-personal-information/>.

companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.¹³

C. How Session Replay Code Works.

22. Session Replay Code, such as that implemented on www.zillow.com, enables website operators to record, save, and replay website visitors' interactions with a given website. The clandestinely deployed code provides online marketers and website designers with insights into the user experience by recording website visitors "as they click, scroll, type or navigate across different web pages."¹⁴

23. While Session Replay Code is utilized by websites for some legitimate purposes, it goes well beyond normal website analytics when it comes to collecting the actual contents of communications between website visitors and websites. Unlike other online advertising tools, Session Replay Code allows a website to capture and record nearly every action a website visitor takes while visiting the website, including actions that reveal the visitor's personal or private sensitive data, sometimes even when the visitor does not intend to submit the data to the website operator, or has not finished submitting the data to the website operator.¹⁵ As a result, website visitors "aren't just sharing data with the [web]site they're on . . . but also with an analytics service that may be watching over their shoulder."¹⁶

¹³ Margaret Taylor, *How Apple screwed Facebook*, Wired, (May 19, 2021), <https://www.wired.co.uk/article/apple-ios14-facebook>.

¹⁴ Erin Gilliam Haije, *[Updated] Are Session Recording Tools a Risk to Internet Privacy?*, Mopinion (Mar. 7, 2018), <https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/>.

¹⁵ *Id.*

¹⁶ Eric Ravenscraft, *Almost Every Website You Visit Records Exactly How Your Mouse Moves*, Medium (Feb. 5, 2020), <https://onezero.medium.com/almost-every-website-you-visit-records-exactly-how-your-mouse-moves-4134cb1cc7a0>.

24. Session Replay Code works by inserting computer code into the various event handling routines that web browsers use to receive input from users, thus intercepting the occurrence of actions the user takes. When a website delivers Session Replay Code to a user's browser, the browser will follow the code's instructions by sending responses in the form of "event" data to a designated third-party server. Typically, the server receiving the event data is controlled by the third-party entity that wrote the Session Replay Code, rather than the owner of the website where the code is installed.

25. The types of events captured by Session Replay Code vary by specific product and configuration, but in general are wide-ranging and can encompass virtually every user action, including all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entry, and numerous other forms of a user's navigation and interaction through the website. In order to permit a reconstruction of a user's visit accurately, the Session Replay Code must be capable of capturing these events at hyper-frequent intervals, often just milliseconds apart. Events are typically accumulated and transmitted in blocks periodically throughout the user's website session, rather than after the user's visit to the website is completely finished.

26. Unless specifically masked through configurations chosen by the website owner, some visible contents of the website may also be transmitted to the Session Replay Provider.

27. Once the events from a user session have been recorded by a Session Replay Code, a website operator can view a visual reenactment of the user's visit through the Session Replay Provider, usually in the form of a video, meaning "[u]nlike typical analytics services that provide

aggregate statistics, these scripts are intended for the recording and playback of individual browsing sessions.”¹⁷

28. Because most Session Replay Codes will by default indiscriminately capture the maximum range of user-initiated events and content displayed by the website, researchers have found that a variety of highly sensitive information can be captured in event responses from website visitors, including medical conditions, credit card details, and other personal information displayed or entered on webpages.¹⁸

29. Most alarming, Session Replay Code may capture data that the user did not even intentionally transmit to a website during a visit, and then make that data available to website owners when they access the session replay through the Session Replay Provider. For example, if a user writes information into a text form field, but then chooses not to click a “submit” or “enter” button on the website, the Session Replay Code may nevertheless cause the non-submitted text to be sent to the designated event-response-receiving server before the user deletes the text or leaves the page. This information will then be viewable to the website owner when accessing the session replay through the Session Replay Provider.

30. Session Replay Code does not necessarily anonymize user sessions, either.

31. First, if a user’s entry of personally identifying information is captured in an event response, that data will become known and visible to both the Session Replay Provider and the website owner.

¹⁷ Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), <https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/>.

¹⁸ *Id.*

32. Second, if a website displays user account information to a logged-in user, that content may be captured by Session Replay Code.

33. Third, some Session Replay Providers explicitly offer website owners cookie functionality that permits linking a session to an identified user, who may be personally identified if the website owner has associated the user with an email address or username.¹⁹

34. Session Replay Providers often create “fingerprints” that are unique to a particular user’s combination of computer and browser settings, screen configuration, and other detectable information. The resulting fingerprint, which is often unique to a user and rarely changes, are collected across all sites that the Session Replay Provider monitors.

35. When a user eventually identifies themselves to one of these websites (such as by filling in a form), the provider can then associate the fingerprint with the user identity and can then back-reference all of that user’s other web browsing across other websites previously visited, including on websites where the user had intended to remain anonymous—even if the user explicitly indicated that they would like to remain anonymous by enabling private browsing.

36. In addition to the privacy invasions caused by the diversion of user communications with websites to third-party Session Replay Providers, Session Replay Code also exposes website visitors to identity theft, online scams, and other privacy threats.²⁰ Indeed, “[t]he more copies of sensitive information that exist, the broader the attack surface, and when data is being collected [

¹⁹ *Id.*; see also *FS.identify – Identifying users*, FullStory, <https://help.fullstory.com/hc/en-us/articles/360020828113>, (last visited Sep. 8, 2022).

²⁰ Juha Sarrinen, *Session Replay is a Major Threat to Privacy on the Web*, itnews (Nov. 16, 2017), <https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720>.

] it may not be stored properly or have standard protections” increasing “the overall risk that data will someday publicly leak or be breached.”²¹

37. Recognizing the privacy concerns posed by Session Replay Code, in 2019 Apple required app developers to remove or properly disclose the use of analytics code that allow app developers to record how a user interacts with their iPhone apps or face immediate removal from the app store.²² In announcing this decision, Apple stated: “Protecting user privacy is paramount in the Apple ecosystem. Our App Store Review Guidelines require that apps request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity.”²³

D. Zillow Secretly Wiretaps its Website Visitors’ Electronic Communications.

38. Zillow operates the website www.zillow.com. Zillow is the “leading online residential real estate” marketplace in the United States for consumers, connecting them to the information and real estate professionals they need to buy, sell, or rent a home.²⁴

39. Zillow has become “synonymous with residential real estate.”²⁵ www.zillow.com is the most popular real estate website in the United States, with over thirty-six million unique

²¹ Lily Hay Newman, *Covert ‘Replay Sessions’ Have Been harvesting Passwords by Mistake*, WIRED (Feb. 26, 2018), <https://www.wired.com/story/covert-replay-sessions-harvesting-passwords/>.

²² Zack Whittaker, *Apple Tells App Developers to Disclose or Remove Screen Recording Code*, TechCrunch (Feb. 7, 2019), <https://techcrunch.com/2019/02/07/apple-glassbox-apps/>.

²³ *Id.*

²⁴ Zillow Group, Inc., *Form 10-K* (Dec. 31, 2021), <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001617640/87bbbf30-39cb-4eb7-acdc-1b51265b9687.pdf> (“Zillow 10-K”).

²⁵ *Id.*

monthly visitors²⁶ and more than 135 million properties are listed on its website.²⁷ According to a 2021 Google Trends report, “[t]oday more people search ‘Zillow’ than ‘real estate.’”²⁸

40. However, unbeknownst to the millions of individuals perusing Zillow’s real estate listings, Zillow intentionally procures and embeds various Session Replay Codes from Session Replay Providers on its website to track and analyze website user interactions with www.zillow.com.

41. One such Session Replay Provider that Zillow procures is Microsoft.

42. Microsoft is the owner and operator of a Session Replay Code titled Clarity, which provides basic information about website user sessions, interactions, and engagement, and breaks down users by device type, county, and other dimensions.²⁹

43. Zillow’s procurement and use of Microsoft Clarity’s Session Replay Code, and procurement and use of other Session Replay Codes through various Session Replay Providers, is a wiretap in violation Pennsylvania statutory and common law.

E. Plaintiff’s and Class Members’ Experience.

44. Plaintiff has visited www.zillow.com on her computer while in Pennsylvania.

45. While visiting Zillow’s website, Plaintiff fell victim to Defendant’s unlawful monitoring, recording, and collection of Plaintiff’s Website Communications with www.zillow.com.

²⁶ *Most Popular Real Estate Websites in the United States as of October 2021, Based on Unique Monthly Visits*, Statista, <https://www.statista.com/statistics/381468/most-popular-real-estate-websites-by-monthly-visits-usa/>, (last visited Sep. 8, 2022).

²⁷ Zillow 10-K, *supra*, note 1.

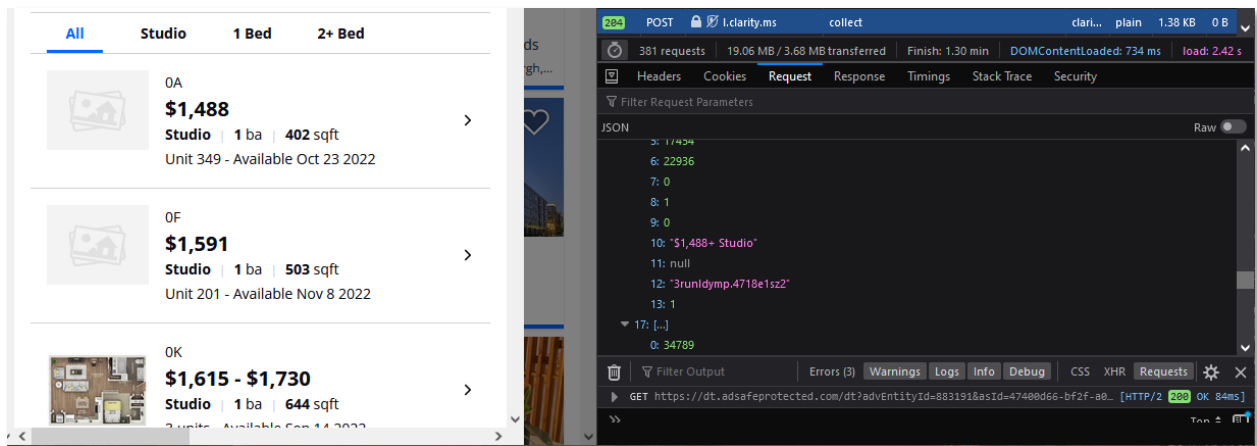
²⁸ *Id.*

²⁹ Jono Alderson, *An Introduction to Microsoft Clarity*, Yoast, <https://yoast.com/introduction-microsoft-clarity/#h-what-is-microsoft-clarity>, (last visited Sep. 8, 2022).

46. Unknown to Plaintiff, Zillow procures and embeds Session Replay Code on its website.

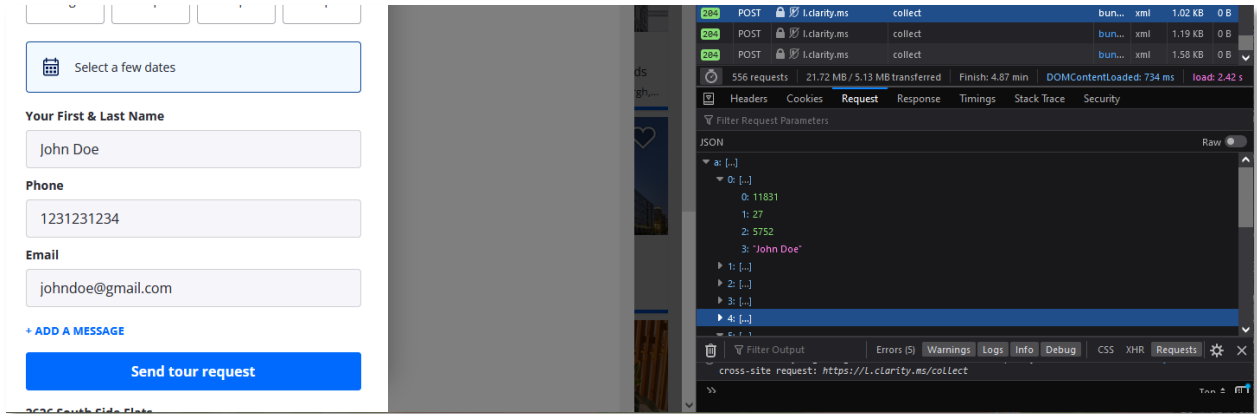
47. During the website visit, Plaintiff's Website Communications were captured by Session Replay Code and sent to various Session Replay Providers.

48. For example, when visiting www.zillow.com, if a website user views a certain piece of property for rent or sale, that information is captured by the Session Replay Codes embedded on the website:



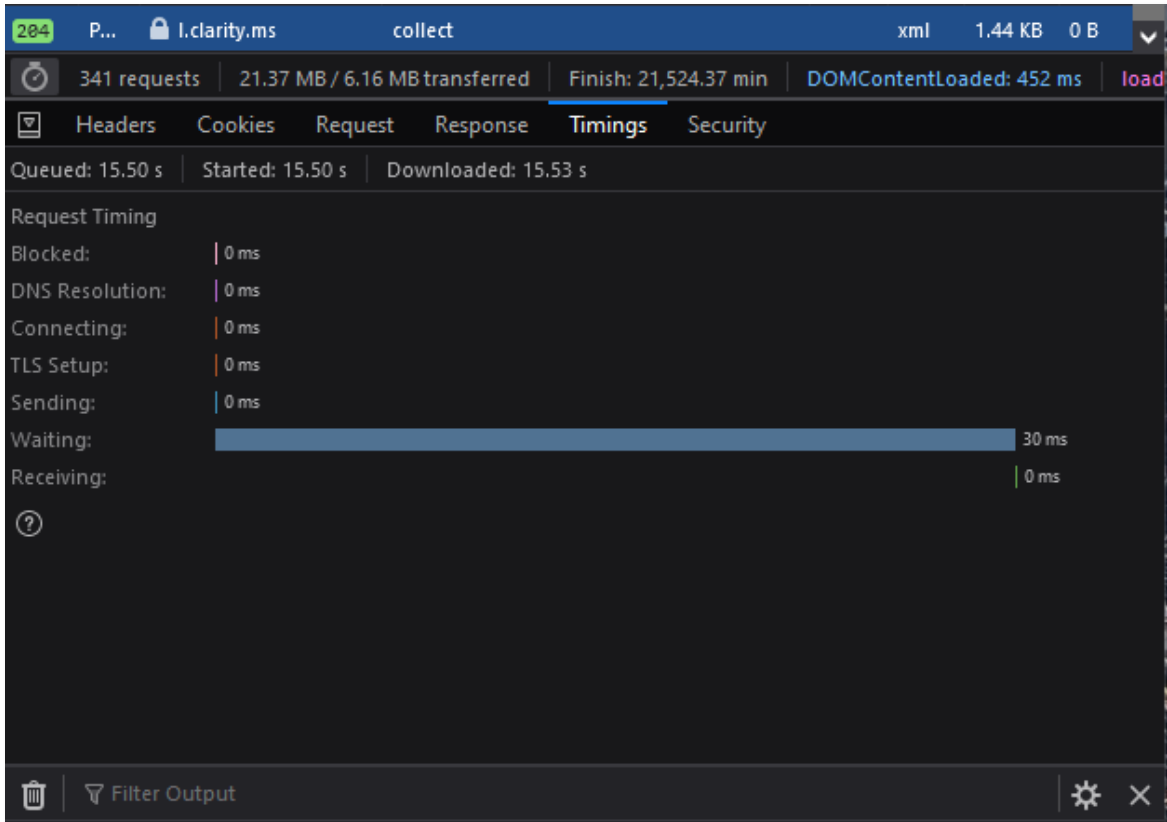
Depicting information sent to one of the Service Replay Providers—Microsoft—through a Service Replay Code—Clarity—after viewing a Studio apartment priced at \$1,488 while visiting www.zillow.com.

49. Similarly, when visiting www.zillow.com, if a user enters personal information in a text box to schedule a tour, that information is captured by the Session Replay Codes embedded on the website:



Depicting information sent to one of the Service Replay Providers—Microsoft—through a Service Replay Code—Clarity—after entering a name (purple text) to a text box to schedule a tour of a property.

50. The wiretapping by the Session Replay Codes are ongoing during the visit and intercepts the contents of these communications between Plaintiff and Zillow with instantaneous transmissions to the Session Replay Provider, as illustrated below, in which only 30 milliseconds were required to send a packet of even response data, which would indicate whatever the website user had just done:



51. The Session Replay Codes operate in the same manner for all putative Class members.

52. Like Plaintiff, each Class member visited www.zillow.com with Session Replay Code embedded in it, and those Session Replay Codes intercepted the Class members' Website Communications with www.zillow.com by sending hyper-frequent logs of those communications to Session Replay Providers.

53. Even if Zillow masks certain elements when it configures the settings of the Session Replay Code embedded on its website, any operational iteration of the Session Replay Code will, by its very nature and purpose, intercept the contents of communications between the website's visitors and the website owner.

54. For example, even with heightened masking enabled, Session Replay Providers will still learn through the intercepted data exactly which pages a user navigates to, how the user moves through the page (such as which areas the user zooms in on or interacted with), and additional substantive information.

55. As a specific example, if a user types a particular address or zip code into Zillow's main search bar and initiates a search, even if the text entered into the search bar is masked, Session Replay Providers will still learn what is entered into the bar as soon as the search result page loads. This is so because the responsive search results will be displayed on the subsequent page, and the responsive content generated by Zillow will repeat the searched information back on the generated page. That information will not be masked even if user-inputted text is fully masked in a text field.

CLASS ACTION ALLEGATIONS

56. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Class:

All natural persons in Pennsylvania whose Website Communications were captured through the use of Session Replay Code embedded in www.zillow.com

57. Excluded from the Class are Defendant, its parents, subsidiaries, affiliates, officers, and directors, all persons who make a timely election to be excluded from the Class, the judge to whom this case is assigned and any immediate family members thereof, and the attorneys who enter their appearance in this action.

58. **Numerosity:** The members of the Class are so numerous that individual joinder of all Class members is impracticable. The precise number of Class members and their identities may be obtained from the books and records of Zillow or the Session Replay Providers.

59. **Commonality:** This action involves questions of law and fact that are common to the Class members. Such common questions include, but are not limited to: (a) whether Defendant

procures Session Replay Providers to intercept Zillow's website visitors' Website Communications; (b) whether Zillow intentionally discloses the intercepted Website Communications of its website users; (c) whether Defendant acquires the contents of website users' Website Communications without their consent; (d) whether Defendant's conduct violates Pennsylvania Wiretap Act, 18 Pa. Cons. Stat. § 5701, *et seq.*; (e) whether Plaintiff and the Class members are entitled to equitable relief; and (f) whether Plaintiff and the Class members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

60. **Typicality:** Plaintiff's claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through the uniform prohibited conduct described above. For instance, Plaintiff and each member of the Class had their communications intercepted in violation of the law and their right to privacy. This uniform injury and the legal theories that underpin recovery make the claims of Plaintiff and the members of the Class typical of one another.

61. **Adequacy of Representation:** Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiff has no interest that is antagonistic to the interests of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiff nor her counsel have any interest adverse to the interests of the other members of the Class.

62. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this

controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

63. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant intercepted Plaintiff's and Class members' Website Communications, then Plaintiff and each Class member suffered damages by that conduct.

64. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class members may be readily identified through Zillow's books and records or the Session Replay Providers' books and records.

COUNT I
Violation of Pennsylvania Wiretap Act
18 Pa. Cons. Stat. § 5701, et. seq.

65. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

66. Plaintiff brings this claim individually and on behalf of the Class.

67. The Pennsylvania Wiretap Act (the "Act") prohibits (1) the interception or procurement of another to intercept any wire, electronic, or oral communication; (2) the intentional disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication; and (3) the intentional use of the contents of any wire, electronic, or oral

communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication. 18 Pa. Cons. Stat. § 5703.

68. Any person who intercepts, discloses, or uses or procures any other person to intercept, disclose, or use, a wire, electronic, or oral communication in violation of the Act is subject to a civil action for (1) actual damages, not less than liquidated damages computed at the rate of \$100/day for each violation or \$1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred. 18 Pa. Cons. Stat. § 5725(a).

69. "Intercept" is defined as any "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." 18 Pa. Cons. Stat. § 5702.

70. "Contents" is defined as "used with respect to any wire, electronic or oral communication, is any information concerning the substance, purport, or meaning of that communication." 18 Pa. Cons. Stat. § 5702.

71. "Person" is defined as "any individual, partnership, association, joint stock company, trust or corporation." 18 Pa. Cons. Stat. § 5702.

72. "Electronic Communication" is defined as "[a]ny transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system." 18 Pa. Cons. Stat. § 5702.

73. Zillow is a person for purposes of the Act because it is a corporation.

74. Session Replay Code like that procured by Zillow is a "device" used for the "acquisition of the contents of any wire, electronic, or oral communication" within the meaning of the Act.

75. Plaintiff's and Class members' intercepted Website Communications constitute the "contents" of electronic communication[s]" within the meaning of the Act.

76. Zillow intentionally procures and embeds Session Replay Code on its website to spy on, automatically and secretly, and intercept its website visitors' electronic interactions communications with Zillow in real time.

77. Plaintiff's and Class members' electronic communications are intercepted contemporaneously with their transmission.

78. Plaintiff and Class members did not consent to having their Website Communications wiretapped.

79. Pursuant to 18 Pa. Cons. Stat. 5725(a), Plaintiff and the Class members seek (1) actual damages, not less than liquidated damages computed at the rate of \$100/day for each violation or \$1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred.

80. Zillow's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT II

Invasion of Privacy – Intrusion Upon Seclusion

81. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

82. Pennsylvania common law recognizes the tort of invasion of privacy. The right to privacy is also embodied in multiple sections of the Pennsylvania constitution.

83. Plaintiff brings this claim individually and on behalf of the Class.

84. Plaintiff and Class members have an objective, reasonable expectation of privacy in their Website Communications.

85. Plaintiff and Class members did not consent to, authorize, or know about Zillow's intrusion at the time it occurred. Plaintiff and Class members never agreed that Zillow could collect or disclose their Website Communications.

86. Plaintiff and Class members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

87. Zillow intentionally intrudes on Plaintiff's and Class members' private life, seclusion, or solitude, without consent.

88. Zillow's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

89. Plaintiff and Class members were harmed by Zillow's wrongful conduct as Zillow's conduct has caused Plaintiff and the Class mental anguish and suffering arising from their loss of privacy and confidentiality of their electronic communications.

90. Zillow's conduct has needlessly harmed Plaintiff and the Class by capturing intimately personal facts and data in the form of their Website Communications. This disclosure and loss of privacy and confidentiality has caused Plaintiff and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

91. Additionally, given the monetary value of individual personal information, Defendant deprived Plaintiff and Class members of the economic value of their interactions with

Defendant's website, without providing proper consideration for Plaintiff's and Class members' property.

92. Further, Zillow has improperly profited from its invasion of Plaintiff and Class members' privacy in its use of their data for its economic value.

93. As a direct and proximate result Zillow's conduct, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

94. Zillow's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

REQUEST FOR RELIEF

Plaintiff, individually and on behalf of the other members of the proposed Class, respectfully request that the Court enter judgment in Plaintiff's and the Class's favor and against Defendant as follows:

- A. Certifying the Class and appointing Plaintiff as the Class representative;
- B. Appointing Plaintiff's counsel as class counsel;
- C. Declaring that Defendant's past conduct was unlawful, as alleged herein;
- D. Declaring Defendant's ongoing conduct is unlawful, as alleged herein;
- E. Enjoining Defendant from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;

F. Awarding Plaintiff and the Class members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

G. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

H. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

I. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the Class, demands a trial by jury of any and all issues in this action so triable of right.

Dated: September 8, 2022

Respectfully submitted,

/s/ Gary F. Lynch

Gary F. Lynch

Kelly K. Iverson

Jamisen A. Etzel

Elizabeth Pollock-Avery

Nicholas A. Colella

Patrick D. Donathen

LYNCH CARPENTER, LLP

1133 Penn Avenue, 5th Floor

Pittsburgh, Pennsylvania 15222

Telephone: 412-322-9243

Facsimile: 412-231-0246

gary@lcllp.com

kelly@lcllp.com

jamisen@lcllp.com

elizabeth@lcllp.com

nickc@lcllp.com

patrick@lcllp.com

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

ASHLEY POPA, individually and on behalf of all others similarly situated,

(b) County of Residence of First Listed Plaintiff Lawrence
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

Gary F. Lynch, Lynch Carpenter, LLP, 1133 Penn Ave,
5th Floor, Pittsburgh, PA 15222 T: 412-322-9243

DEFENDANTS

ZILLOW GROUP, INC.

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff
☐ 2 U.S. Government Defendant
☐ 3 Federal Question (U.S. Government Not a Party)
☒ 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- | | PTF | DEF | | PTF | DEF |
|---|---------------------------------------|----------------------------|---|----------------------------|---------------------------------------|
| Citizen of This State | <input checked="" type="checkbox"/> 1 | <input type="checkbox"/> 1 | Incorporated or Principal Place of Business In This State | <input type="checkbox"/> 4 | <input type="checkbox"/> 4 |
| Citizen of Another State | <input type="checkbox"/> 2 | <input type="checkbox"/> 2 | Incorporated and Principal Place of Business In Another State | <input type="checkbox"/> 5 | <input checked="" type="checkbox"/> 5 |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3 | <input type="checkbox"/> 3 | Foreign Nation | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 |

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Click here for: [Nature of Suit Code Descriptions.](#)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input checked="" type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice PERSONAL INJURY <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act IMMIGRATION <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 PROPERTY RIGHTS <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 835 Patent - Abbreviated New Drug Application <input type="checkbox"/> 840 Trademark <input type="checkbox"/> 880 Defend Trade Secrets Act of 2016 SOCIAL SECURITY <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit (15 USC 1681 or 1692) <input type="checkbox"/> 485 Telephone Consumer Protection Act <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
REAL PROPERTY <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	CIVIL RIGHTS <input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education PRISONER PETITIONS Habeas Corpus: <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty Other: <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN (Place an "X" in One Box Only)

- ☒ 1 Original Proceeding
☐ 2 Removed from State Court
☐ 3 Remanded from Appellate Court
☐ 4 Reinstated or Reopened
☐ 5 Transferred from Another District (specify)
☐ 6 Multidistrict Litigation - Transfer
☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
28 U.S.C. § 1332(d)

Brief description of cause:
Violation of PA Wiretap Act and invasion of privacy

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P. DEMAND \$

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE _____ DOCKET NUMBER _____

DATE

SIGNATURE OF ATTORNEY OF RECORD

9/8/2022

/s/ Gary F. Lynch

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

JS 44A REVISED June, 2009
IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF PENNSYLVANIA
THIS CASE DESIGNATION SHEET MUST BE COMPLETED

PART A

This case belongs on the (☐ Erie ☐ Johnstown ☒ Pittsburgh) calendar.

1. **ERIE CALENDAR** - If cause of action arose in the counties of Crawford, Elk, Erie, Forest, McKean, Venang or Warren, OR any plaintiff or defendant resides in one of said counties.
2. **JOHNSTOWN CALENDAR** - If cause of action arose in the counties of Bedford, Blair, Cambria, Clearfield or Somerset OR any plaintiff or defendant resides in one of said counties.
3. Complete if on **ERIE CALENDAR**: I certify that the cause of action arose in _____ County and that the _____ resides in _____ County.
4. Complete if on **JOHNSTOWN CALENDAR**: I certify that the cause of action arose in _____ County and that the _____ resides in _____ County.

PART B (You are to check ONE of the following)

1. ☐ This case is related to Number _____. Short Caption _____.
2. ☒ This case is not related to a pending or terminated case.

DEFINITIONS OF RELATED CASES:

CIVIL: Civil cases are deemed related when a case filed relates to property included in another suit or involves the same issues of fact or it grows out of the same transactions as another suit or involves the validity or infringement of a patent involved in another suit
EMINENT DOMAIN: Cases in contiguous closely located groups and in common ownership groups which will lend themselves to consolidation for trial shall be deemed related.

HABEAS CORPUS & CIVIL RIGHTS: All habeas corpus petitions filed by the same individual shall be deemed related. All pro se Civil Rights actions by the same individual shall be deemed related.

PART C

I. CIVIL CATEGORY (Select the applicable category).

1. ☐ Antitrust and Securities Act Cases
2. ☐ Labor-Management Relations
3. ☐ Habeas corpus
4. ☐ Civil Rights
5. ☐ Patent, Copyright, and Trademark
6. ☐ Eminent Domain
7. ☐ All other federal question cases
8. ☒ All personal and property damage tort cases, including maritime, FELA, Jones Act, Motor vehicle, products liability, assault, defamation, malicious prosecution, and false arrest
9. ☐ Insurance indemnity, contract and other diversity cases.
10. ☐ Government Collection Cases (shall include HEW Student Loans (Education), V A Overpayment, Overpayment of Social Security, Enlistment Overpayment (Army, Navy, etc.), HUD Loans, GAO Loans (Misc. Types), Mortgage Foreclosures, SBA Loans, Civil Penalties and Coal Mine Penalty and Reclamation Fees.)

I certify that to the best of my knowledge the entries on this Case Designation Sheet are true and correct

/s/ Gary F. Lynch

Date: 9/8/2022

ATTORNEY AT LAW

NOTE: ALL SECTIONS OF BOTH FORMS MUST BE COMPLETED BEFORE CASE CAN BE PROCESSED.

U.S. District Court
Western District of Pennsylvania (Pittsburgh)
CIVIL DOCKET FOR CASE #: 2:22-cv-01287-WSS

POPA v. ZILLOW GROUP, INC.
Assigned to: Judge William S. Stickman
Cause: 28:1332 Diversity-Other Contract

Date Filed: 09/08/2022
Jury Demand: Plaintiff
Nature of Suit: 190 Contract: Other
Jurisdiction: Diversity

Plaintiff

ASHLEY POPA
individually and on behalf of all others
similarly situated

represented by **Gary F. Lynch**
Lynch Carpenter, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
412-322-9243
Email: Gary@lcllp.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Elizabeth Pollock-Avery
Lynch Carpenter, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
412-322-9243
Email: Elizabeth@lcllp.com
ATTORNEY TO BE NOTICED

V.

Defendant

ZILLOW GROUP, INC.

represented by **Samantha Southall**
Buchanan Ingersoll & Rooney PC
Two Liberty Place
50 S. 16th Street
Ste 3200
Philadelphia, PA 19063
215-665-8700
Fax: 215-665-8760
Email: samantha.southall@bipc.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
09/08/2022	<u>1</u>	COMPLAINT against ZILLOW GROUP, INC. (Filing fee, including Administrative fee, \$402, receipt number : APAWDC-7281749), filed by ASHLEY POPA. (Attachments: # <u>1</u> Civil Cover Sheet) (jd) (Entered: 09/08/2022)
09/08/2022	<u>2</u>	Summons Issued as to ZILLOW GROUP, INC. (jd) (Entered: 09/08/2022)
09/23/2022	<u>3</u>	SUMMONS/Return of Service Returned Executed by ASHLEY POPA. ZILLOW GROUP,

		INC. served on 9/12/2022, answer due 10/3/2022. (Lynch, Gary) (Entered: 09/23/2022)
09/29/2022	4	Stipulation for Extension of Time to Answer by ZILLOW GROUP, INC. Answer due from ZILLOW GROUP, INC.. (Southall, Samantha) (Entered: 09/29/2022)
09/29/2022	5	Proposed Order re 4 Stipulation for Extension of Time to Answer <i>Move or Otherwise Respond to Plaintiff's Complaint</i> by ZILLOW GROUP, INC.. (Southall, Samantha) (Entered: 09/29/2022)
09/29/2022	6	ORDER APPROVING 4 Stipulation for Extension of Time to Answer. The Parties' Stipulation to Extend Time for Defendant Zillow Group, Inc. to Answer, Move or Otherwise Respond to Plaintiff's Complaint is APPROVED. Defendant Zillow Group, Inc. shall have an extension of thirty (30) days, from October 3, 2022, until November 2, 2022, to answer, move or otherwise respond to Plaintiff's Complaint. Signed by Judge William S. Stickman on 09/29/22. Text-only entry; no PDF document will issue. This text-only entry constitutes the Order of the Court or Notice on the matter. (eca) (Entered: 09/29/2022)
09/30/2022	7	NOTICE of Appearance by Samantha Southall on behalf of ZILLOW GROUP, INC.. (Southall, Samantha) (Entered: 09/30/2022)
09/30/2022	8	NOTICE of Appearance by Elizabeth Pollock-Avery on behalf of ASHLEY POPA. (Pollock-Avery, Elizabeth) (Entered: 09/30/2022)

PACER Service Center			
Transaction Receipt			
10/19/2022 11:43:49			
PACER Login:	samanthasouthall	Client Code:	0106198-000001-SS
Description:	Docket Report	Search Criteria:	2:22-cv-01287-WSS
Billable Pages:	2	Cost:	0.20

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI**

JILL ADAMS and JILL ADAMS as Natural
Mother and Next Friend of her minor child,
H.A., individually and on behalf of all others
similarly situated,

Plaintiff,

v.

ZILLOW GROUP, INC.,

Defendant.

Case No. 4:22-cv-1023

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Jill Adams and Jill Adams as Natural Mother and Next Friend of her minor child, H.A. (collectively referred to as “Plaintiff”), individually and on behalf of all others similarly situated, hereby files this class action complaint against Defendant Zillow Group, Inc. (“Defendant” or “Zillow”), and in support thereof alleges the following:

INTRODUCTION

1. This is a class action brought against Zillow for surreptitiously intercepting the private electronic communications of visitors to its website, www.zillow.com, without their consent. Zillow knowingly directs third-party vendors, such as Microsoft Corporation, to embed snippets of JavaScript computer code (“Session Replay Code”) on Zillow’s website, which then deploys on each website visitor’s internet browser for the purpose intercepting and recording the website visitor’s private electronic communications with the Zillow website, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time (“Website Communications”). These third-party vendors (collectively, “Session Replay Providers”) create

and deploy the Session Replay Code at Zillow’s request.

2. After intercepting and recording the Website Communications, Zillow and the Session Replay Providers use those Website Communications to recreate website visitors’ entire visit to www.zillow.com. The Session Replay Providers create a video replay of the user’s behavior on the website and provide it to Zillow for analysis. Zillow’s directive to the Session Replay Providers to secretly deploy the Session Replay Code results in the electronic equivalent of “looking over the shoulder” of each visitor to the Zillow website for the entire duration of their website interaction.

3. Zillow’s conduct violates the Missouri Wiretap Act, Mo. Ann. Stat. §§ 542.400 *et seq.*, the Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.010 *et seq.*, and constitutes an invasion of the privacy rights of website visitors.

4. Plaintiff brings this action individually and on behalf of a class of all Missouri citizens whose Website Communications were intercepted at Zillow’s direction and use of Session Replay Code embedded on the webpages of www.zillow.com and seeks all civil remedies provided under the causes of action, including but not limited to compensatory, statutory, and/or punitive damages, and attorneys’ fees and costs.

PARTIES

5. Plaintiff Jill Adams, herself and as Natural Mother and Next Friend of her minor child, H.A., is a citizen of the state of Missouri, and at all times relevant to this action, resided and was domiciled in Saint Louis County, Missouri.

6. Plaintiff Jill Adams’ minor child, H.A., is a citizen of the state of Missouri, and at all times relevant to this action, resided and was domiciled in Saint Louis County, Missouri.

7. Plaintiff Jill Adams has consented to serve as next friend of minor, H.A.

8. Defendant Zillow Group, Inc. is corporation organized under the laws of Washington, and its principal place of business is located at 1301 Second Ave., Floor 31, Seattle Washington, 98101. Defendant is a citizen of Washington.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of \$5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class, including Plaintiff, is a citizen of a state different than Defendant.

10. This Court has personal jurisdiction over Defendant because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in Missouri. The privacy violations complained of herein resulted from Defendant's purposeful and tortious acts directed towards citizens of Missouri while they were located within Missouri. At all relevant times, Defendant knew that its practices would directly result in collection of information from Missouri citizens while those citizens browse www.zillow.com. Defendant chose to avail itself of the business opportunities of making its real property and rental advertising services specifically available in Missouri (and specifically with respect to Missouri properties) and collecting real-time data from website visit sessions initiated by Missourians while located in Missouri, and the claims alleged herein arise from those activities.

11. Zillow also knows that many users visit and interact with Zillow's websites while they are physically present in Missouri. Both desktop and mobile versions of Zillow's website allow a user to search for nearby properties by providing the user's "current location," as furnished by the location-determining tools of the device the user is using or by the user's IP address (*i.e.*,

without requiring the user to manually input an address), as does the Zillow App. Users' employment of automatic location services in this way means that Zillow is continuously made aware that its website is being visited by people located in Missouri, and that such website visitors are being eavesdropped on in violation Missouri statutory and common law.

12. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

FACTUAL ALLEGATIONS

A. Website User and Usage Data Have Immense Economic Value.

13. The "world's most valuable resource is no longer oil, but data."¹

14. Earlier this year, Business News Daily reported that some businesses collect personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data (*i.e.*, how consumers interact with a business's website, applications, and emails), behavioral data (*i.e.*, customers' purchase histories and product usage information), and attitudinal data (*i.e.*, data on consumer satisfaction) from consumers.² This information is valuable to companies because they can use this data to improve customer experiences, refine their marketing strategies, capture data to sell it, and even to secure more sensitive consumer data.³

15. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business's success.

¹ *The world's most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

² Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, Business News Daily (Aug. 5, 2022), <https://www.businessnewsdaily.com/10625-businesses-collecting-data.html>.

³ *Id.*

Research shows that organizations who “leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin.”⁴

16. In 2013, the Organization for Economic Cooperation and Development (“OECD”) even published a paper entitled “Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value.”⁵ In this paper, the OECD measured prices demanded by companies concerning user data derived from “various online data warehouses.”⁶

17. OECD indicated that “[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e. \$2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver’s license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55.”⁷

B. Website Users Have a Reasonable Expectation of Privacy in Their Interactions with Websites.

18. Consumers are skeptical and are wary about their data being collected. A report released by KPMG shows that “a full 86% of the respondents said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected.”⁸

19. Another recent paper also indicates that most website visitors will assume their

⁴ Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), <https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data>.

⁵ Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), <https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf>.

⁶ *Id.* at 25.

⁷ *Id.*

⁸ Lance Whitney, *Data privacy is a growing concern for more consumers*, TechRepublic (Aug. 17, 2021), <https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/>.

detailed interactions with a website will only be used by the website and not be shared with a party they know nothing about.⁹ As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.¹⁰

20. Privacy polls and studies show that a majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

21. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.¹¹

22. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.¹²

23. Users act consistently with their expectation of privacy. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not

⁹ *CUJO AI Recent Survey Reveals U.S. Internet Users Expectations and Concerns Towards Privacy and Online Tracking*, CUJO (May 26, 2020), <https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html>.

¹⁰ Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, *The Information Society*, 38:4, 257, 258 (2022).

¹¹ *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, Consumer Reports (May 11, 2017), <https://www.consumerreports.org/consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/>.

¹² *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, (Nov. 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confusedand-feeling-lack-of-control-over-their-personal-information/>.

to allow such tracking.¹³

C. How Session Replay Code Works.

24. Session Replay Code, such as that implemented on www.zillow.com, enables website operators to record, save, and replay website visitors' interactions with a given website. The clandestinely deployed code provides online marketers and website designers with insights into the user experience by recording website visitors "as they click, scroll, type or navigate across different web pages."¹⁴

25. While Session Replay Code is utilized by websites for some legitimate purposes, it goes well beyond normal website analytics when it comes to collecting the actual contents of communications between website visitors and websites. Unlike other online advertising tools, Session Replay Code allows a website to capture and record nearly every action a website visitor takes while visiting the website, including actions that reveal the visitor's personal or private sensitive data, sometimes even when the visitor does not intend to submit the data to the website operator, or has not finished submitting the data to the website operator.¹⁵ As a result, website visitors "aren't just sharing data with the [web]site they're on . . . but also with an analytics service that may be watching over their shoulder."¹⁶

26. Session Replay Code works by inserting computer code into the various event handling routines that web browsers use to receive input from users, thus intercepting the

¹³ Margaret Taylor, *How Apple screwed Facebook*, Wired, (May 19, 2021), <https://www.wired.co.uk/article/apple-ios14-facebook>.

¹⁴ Erin Gilliam Haije, *[Updated] Are Session Recording Tools a Risk to Internet Privacy?*, Mopinion (Mar. 7, 2018), <https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/>.

¹⁵ *Id.*

¹⁶ Eric Ravenscraft, *Almost Every Website You Visit Records Exactly How Your Mouse Moves*, Medium (Feb. 5, 2020), <https://onezero.medium.com/almost-every-website-you-visit-records-exactly-how-your-mouse-moves-4134cb1cc7a0>.

occurrence of actions the user takes. When a website delivers Session Replay Code to a user's browser, the browser will follow the code's instructions by sending responses in the form of "event" data to a designated third-party server. Typically, the server receiving the event data is controlled by the third-party entity that wrote the Session Replay Code, rather than the owner of the website where the code is installed.

27. The types of events captured by Session Replay Code vary by specific product and configuration, but in general are wide-ranging and can encompass virtually every user action, including all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entry, and numerous other forms of a user's navigation and interaction through the website. In order to permit a reconstruction of a user's visit accurately, the Session Replay Code must be capable of capturing these events at hyper-frequent intervals, often just milliseconds apart. Events are typically accumulated and transmitted in blocks periodically throughout the user's website session, rather than after the user's visit to the website is completely finished.

28. Unless specifically masked through configurations chosen by the website owner, some visible contents of the website may also be transmitted to the Session Replay Provider.

29. Once the events from a user session have been recorded by a Session Replay Code, a website operator can view a visual reenactment of the user's visit through the Session Replay Provider, usually in the form of a video, meaning "[u]nlike typical analytics services that provide aggregate statistics, these scripts are intended for the recording and playback of individual browsing sessions."¹⁷

30. Because most Session Replay Codes will by default indiscriminately capture the

¹⁷ Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), <https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/>.

maximum range of user-initiated events and content displayed by the website, researchers have found that a variety of highly sensitive information can be captured in event responses from website visitors, including medical conditions, credit card details, and other personal information displayed or entered on webpages.¹⁸

31. Most alarming, Session Replay Code may capture data that the user did not even intentionally transmit to a website during a visit, and then make that data available to website owners when they access the session replay through the Session Replay Provider. For example, if a user writes information into a text form field, but then chooses not to click a “submit” or “enter” button on the website, the Session Replay Code may nevertheless cause the non-submitted text to be sent to the designated event-response-receiving server before the user deletes the text or leaves the page. This information will then be viewable to the website owner when accessing the session replay through the Session Replay Provider.

32. Session Replay Code does not necessarily anonymize user sessions, either.

33. First, if a user’s entry of personally identifying information is captured in an event response, that data will become known and visible to both the Session Replay Provider and the website owner.

34. Second, if a website displays user account information to a logged-in user, that content may be captured by Session Replay Code.

35. Third, some Session Replay Providers explicitly offer website owners cookie functionality that permits linking a session to an identified user, who may be personally identified if the website owner has associated the user with an email address or username.¹⁹

¹⁸ *Id.*

¹⁹ *Id.*; see also *FS.identify – Identifying users*, FullStory, <https://help.fullstory.com/hc/en-us/articles/360020828113>, (last visited Sep. 8, 2022).

36. Session Replay Providers often create “fingerprints” that are unique to a particular user’s combination of device and browser settings, screen configuration, and other detectable information. The resulting fingerprint, which is often unique to a user and rarely changes, are collected across all sites that the Session Replay Provider monitors.

37. When a user eventually identifies themselves to one of these websites (such as by filling in a form), the provider can then associate the fingerprint with the user identity and can then back-reference all of that user’s other web browsing across other websites previously visited, including on websites where the user had intended to remain anonymous—even if the user explicitly indicated that they would like to remain anonymous by enabling private browsing.

38. In addition to the privacy invasions caused by the diversion of user communications with websites to third-party Session Replay Providers, Session Replay Code also exposes website visitors to identity theft, online scams, and other privacy threats.²⁰ Indeed, “[t]he more copies of sensitive information that exist, the broader the attack surface, and when data is being collected [] it may not be stored properly or have standard protections” increasing “the overall risk that data will someday publicly leak or be breached.”²¹

39. Recognizing the privacy concerns posed by Session Replay Code, in 2019 Apple required app developers to remove or properly disclose the use of analytics code that allow app developers to record how a user interacts with their iPhone apps or face immediate removal from

²⁰ Juha Sarrinen, *Session Replay is a Major Threat to Privacy on the Web*, itnews (Nov. 16, 2017), <https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720>.

²¹ Lily Hay Newman, *Covert ‘Replay Sessions’ Have Been harvesting Passwords by Mistake*, WIRED (Feb. 26, 2018), <https://www.wired.com/story/covert-replay-sessions-harvesting-passwords/>.

the app store.²² In announcing this decision, Apple stated: “Protecting user privacy is paramount in the Apple ecosystem. Our App Store Review Guidelines require that apps request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity.”²³

D. Zillow Secretly Eavesdrops on its Website Visitors’ Electronic Communications.

40. Zillow operates the website www.zillow.com. Zillow is the “leading online residential real estate” marketplace in the United States for consumers, connecting them to the information and real estate professionals they need to buy, sell, or rent a home.²⁴

41. Zillow has become “synonymous with residential real estate.”²⁵ www.zillow.com is the most popular real estate website in the United States, with over thirty-six million unique monthly visitors²⁶ and more than 135 million properties are listed on its website.²⁷ According to a 2021 Google Trends report, “[t]oday more people search ‘Zillow’ than ‘real estate.’”²⁸

42. However, unbeknownst to the millions of individuals perusing Zillow’s real estate listings, Zillow knowingly directs Session Replay Providers to embed various Session Replay Codes on its website to track and analyze website user interactions with www.zillow.com. Because the Session Replay Providers are unknown eavesdroppers to visitors to www.zillow.com, they are

²² Zack Whittaker, *Apple Tells App Developers to Disclose or Remove Screen Recording Code*, TechCrunch (Feb. 7, 2019), <https://techcrunch.com/2019/02/07/apple-glassbox-apps/>.

²³ *Id.*

²⁴ Zillow Group, Inc., *Form 10-K* (Dec. 31, 2021), <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001617640/87bbbf30-39cb-4eb7-acdc-1b51265b9687.pdf> (“Zillow 10-K”).

²⁵ *Id.*

²⁶ *Most Popular Real Estate Websites in the United States as of October 2021, Based on Unique Monthly Visits*, Statista, <https://www.statista.com/statistics/381468/most-popular-real-estate-websites-by-monthly-visits-usa/>, (last visited Sep. 8, 2022).

²⁷ Zillow 10-K, *supra*, note 1.

²⁸ *Id.*

not parties to website visitors' Website Communications with Zillow.

43. One such Session Replay Provider that Zillow procures is Microsoft.

44. Microsoft is the owner and operator of a Session Replay Code titled Clarity, which provides basic information about website user sessions, interactions, and engagement, and breaks down users by device type, county, and other dimensions.²⁹

45. Zillow knowingly derives a benefit and/or information from the Website Communications intercepted and recorded at its direction. Upon information and belief, Zillow uses the intercepted Website Communications to replay website visitors' interactions with www.zillow.com, improve user interactions with its website, and to provide targeted real estate advertisements to its website visitors.

46. Zillow's knowing direction and use of Microsoft Clarity's Session Replay Code, direction and use of other Session Replay Codes through various Session Replay Providers, and its knowing derivation of a benefit and/or information from the Website Communications surreptitiously intercepted and recorded by Session Replay Codes is a violation of Missouri statutory and common law.

E. Plaintiffs' and Class Members' Experience.

47. Plaintiff has visited www.zillow.com on their respective devices while in Missouri. Specifically, Plaintiff Jill Adams visited www.zillow.com via the web browser on both her mobile phone and computer, and also used the Zillow App on her mobile phone. Plaintiff's minor child, H.A., visited www.zillow.com via the web browser on her phone.

48. While visiting Zillow's website, Plaintiff fell victim to Defendant's unlawful

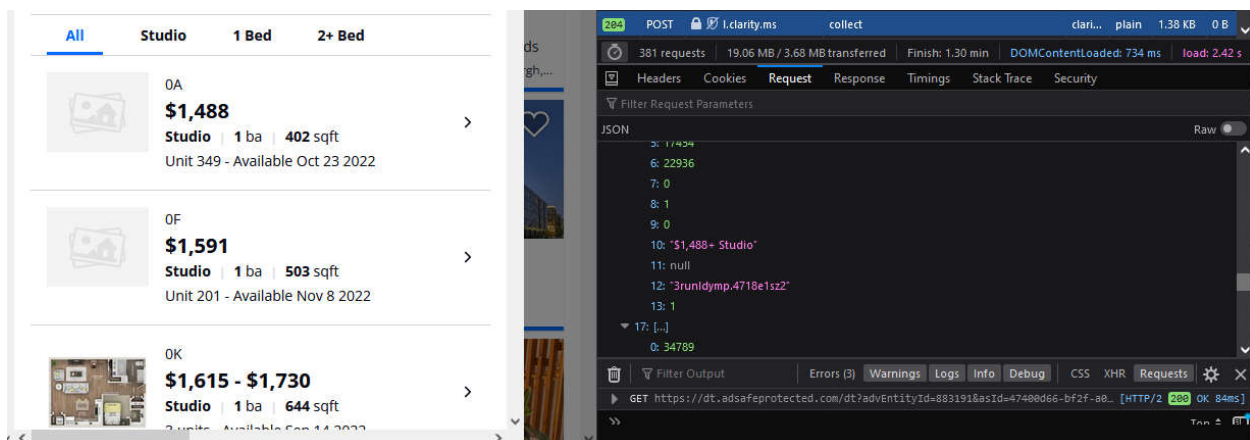
²⁹ Jono Alderson, *An Introduction to Microsoft Clarity*, Yoast, <https://yoast.com/introduction-microsoft-clarity/#h-what-is-microsoft-clarity>, (last visited Sep. 8, 2022).

monitoring, recording, and collection of Plaintiff's Website Communications with www.zillow.com.

49. Unknown to Plaintiff, Zillow directs Session Replay Providers to embed Session Replay Code on its website.

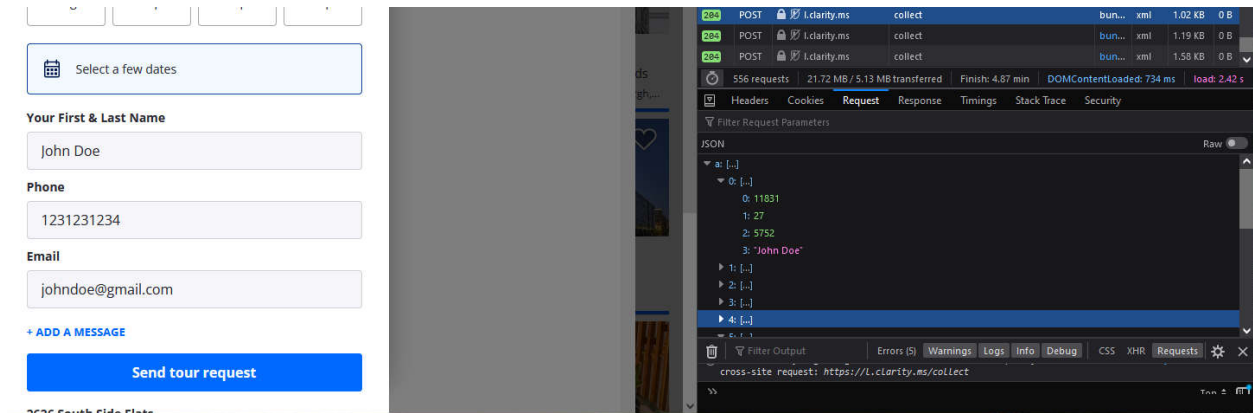
50. During the website visit, Plaintiff's Website Communications were captured by Session Replay Code and sent to various Session Replay Providers.

51. For example, when visiting www.zillow.com, if a website user views a certain piece of property for rent or sale, that information is captured by the Session Replay Codes embedded on the website:



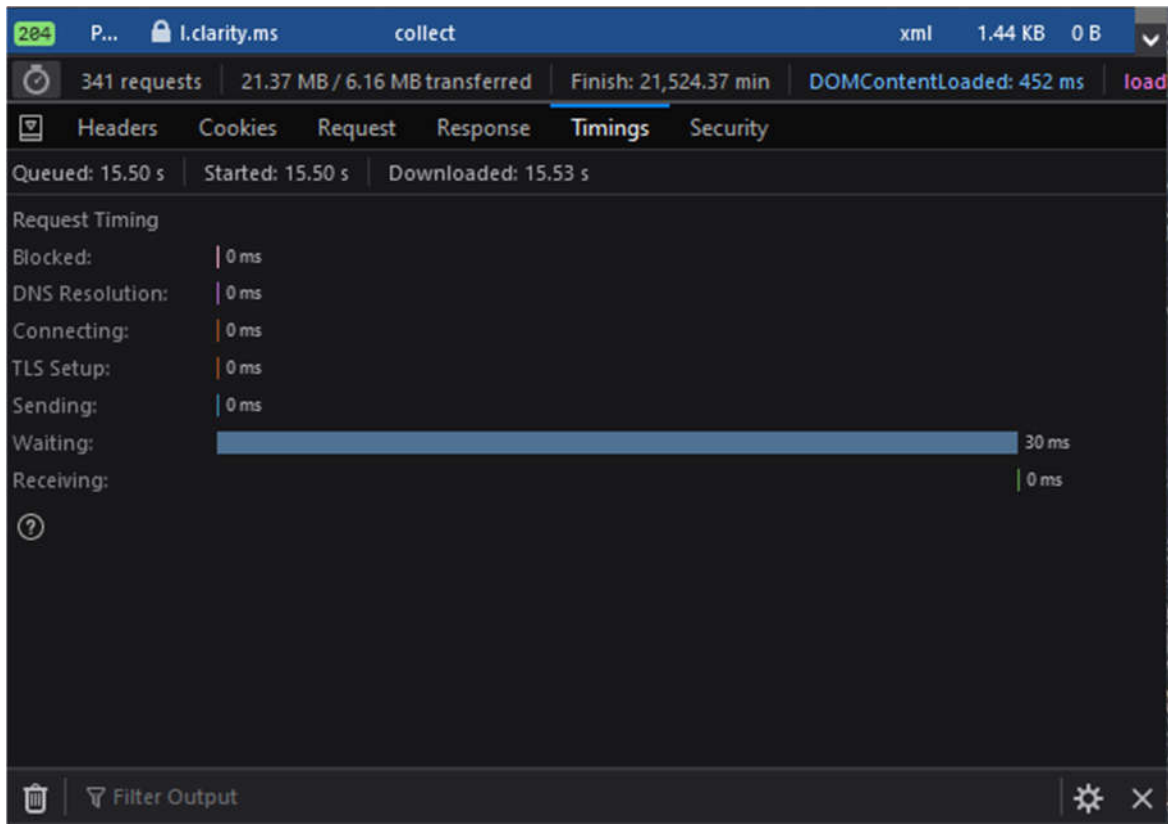
Depicting information sent to one of the Service Replay Providers—Microsoft—through a Service Replay Code—Clarity—after viewing a Studio apartment priced at \$1,488 while visiting www.zillow.com.

52. Similarly, when visiting www.zillow.com, if a user enters personal information in a text box to schedule a tour, that information is captured by the Session Replay Codes embedded on the website:



Depicting information sent to one of the Service Replay Providers—Microsoft—through a Service Replay Code—Clarity—after entering a name (purple text) to a text box to schedule a tour of a property.

53. The eavesdropping by the Session Replay Code is ongoing during the visit and they intercept the contents of these communications between Plaintiff and Zillow with instantaneous transmissions to the Session Replay Providers, as illustrated below, in which only 30 milliseconds were required to send a packet of event response data, which would indicate whatever the website user had just done:



54. The Session Replay Codes operate in the same manner for all putative Class members.

55. Like Plaintiff, each member of the Classes visited www.zillow.com with Session Replay Code embedded in it, and those Session Replay Codes intercepted the members of the Classes' Website Communications with www.zillow.com by sending hyper-frequent logs of those communications to Session Replay Providers.

56. Even if Zillow masks certain elements when it configures the settings of the Session Replay Code embedded on its website, any operational iteration of the Session Replay Code will, by its very nature and purpose, intercept the contents of communications between the website's visitors and the website owner.

57. For example, even with heightened masking enabled, Session Replay Providers will still learn through the intercepted data exactly which pages a user navigates to, how the user moves

through the page (such as which areas the user zooms in on or interacted with), and additional substantive information.

58. As a specific example, if a user types a particular address or zip code into Zillow’s main search bar and initiates a search, even if the text entered into the search bar is masked, Session Replay Providers will still learn what is entered into the bar as soon as the search result page loads. This is so because the responsive search results will be displayed on the subsequent page, and the responsive content generated by Zillow will repeat the searched information back on the generated page. That information will not be masked even if user-inputted text is fully masked in a text field.

CLASS ACTION ALLEGATIONS

59. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Class:

All natural persons in the State of Missouri whose Website Communications were captured through the use of Session Replay Code embedded in www.zillow.com.

60. Plaintiff also brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Subclass:

All natural persons in the State of Missouri who were minors at the time their Website Communications were captured through the use of Session Replay Code embedded in www.zillow.com.

61. The Subclass is the “Minor Subclass;” both the class and subclass are collectively referred to as the “Classes.”

62. Excluded from the Classes are Defendant, its parents, subsidiaries, affiliates, officers, and directors, all persons who make a timely election to be excluded from the Classes, the judge to whom this case is assigned and any immediate family members thereof, and the attorneys who enter their appearance in this action.

63. Plaintiff reserves the right to expand, limit, modify, or amend the Class and

Subclass definition, including the addition of one or more subclasses, in connection with Plaintiff's motion for class certification, or at any other time, based upon, *inter alia*, changing circumstances and/or new facts obtained during discovery.

64. **Numerosity:** The members of the Classes are so numerous that individual joinder of all members of the Classes is impracticable. The precise number of members of the Classes and their identities may be obtained from the books and records of Zillow or the Session Replay Providers.

65. **Commonality:** This action involves questions of law and fact that are common to the members of the Classes. Such common questions include, but are not limited to: (a) whether Defendant employed Session Replay Providers to intercept and record Zillow's website visitors' Website Communications; (b) whether Defendant operated or participated in the operation of an eavesdropping device; (c) whether Defendant derives a benefit or information from the illegal use of an eavesdropping device; (d) whether Defendant directed another to use an eavesdropping device illegally on its behalf; (e) whether Session Replay Code is an "eavesdropping device" used to intercept or record private electronic communications; (f) whether Defendant acquired the contents of website users' private electronic communications without their consent; (g) whether Plaintiff and members of the Classes had a reasonable expectation of privacy in their Website communications; (f) whether Defendant violated the Missouri Wiretap Act, Mo. Ann. Stat. §§ 542.400 *et seq.*; (g) whether Defendant's interception of Plaintiff's and Class and Subclass members' private electronic communications is an unfair or deceptive act or practice; (h) whether Zillow's conduct violates the Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.010 *et seq.* (i) whether Plaintiff and the members of the Classes are entitled to equitable relief; and (j) whether Plaintiff and the members of the Classes are entitled to actual, statutory, punitive, or other

forms of damages, and other monetary relief.

66. **Typicality:** Plaintiff's claims are typical of the other Class and Subclass members' claims because, among other things, all members of the Classes were comparably injured through the uniform prohibited conduct described above. For instance, Plaintiff and each member of the Classes had their electronic communications intercepted in violation of the law and their right to privacy. This uniform injury and the legal theories that underpin recovery make the claims of Plaintiff and the members of the Classes typical of one another.

67. **Adequacy of Representation:** Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Classes. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiff has no interest that is antagonistic to the interests of the Classes, and Defendant has no defenses unique to any Plaintiff. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the members of the Classes, and they have the resources to do so. Neither Plaintiff nor her counsel have any interest adverse to the interests of the other members of the Classes.

68. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Classes is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

69. **Predominance:** Common questions of law and fact predominate over any

questions affecting only individual members of the Classes. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Classes. If Defendant intercepted Plaintiff's and Class and Subclass members' Website Communications, then Plaintiff and each Class and Subclass member suffered damages by that conduct.

70. **Ascertainability:** Members of the Classes are ascertainable. Class membership is defined using objective criteria and members of the Classes may be readily identified through Zillow's books and records or the Session Replay Providers' books and records.

COUNT I
Violation of Missouri Wiretap Act,
Mo. Ann. Stat. §§ 542.400 *et seq.*

71. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

72. Plaintiff brings this claim individually and on behalf of the Classes.

73. The Missouri wiretap statute broadly prohibits the interception, disclosure or use of any wire, oral or electronic communication. Mo. Stat. § 542.402.

74. Any person whose wire communication is intercepted, disclosed, or used in violation of sections 542.00 to 542.422 shall (1) have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications; and (2) be entitled to recover from any such person: (a) actual damages, but not less than liquidated damages computed at the rate of one hundred dollars a day for each day of violation or ten thousand dollars whichever is greater; (b) punitive damages on a showing of a willful or intentional violation of sections 542.400 to 542.422; and (c) A reasonable attorney's fee

and other litigation costs reasonably incurred. Mo. Stat. § 542.218.

75. “Wire communication” is defined as “any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception including the use of such connection in a switching station furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of local, state or interstate communications.” Mo. Stat. § 542.200(12).

76. A “Person” is “defined as any employee, or agent of this state or political subdivision of this state, and any individual, partnership, association, joint stock company, trust, or corporation.” Mo. Stat. § 542.200(9).

77. “Intercept” is defined as “the aural acquisition of the contents of any wire communication through the use of any electronic or mechanical device, including but not limited to interception by one spouse of another spouse.” Mo. Stat. § 542.200(6).

78. “Electronic, mechanical, or other device” is defined as “any device or apparatus which can be used to intercept a wire communication other than: (a) Any telephone or telegraph instrument, equipment or facility, or any component thereof, owned by the user or furnished to the subscriber or user by a communications common carrier in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or being used by a communications common carrier in the ordinary course of its business or by an investigative office or law enforcement officer in the ordinary course of his duties; or (b) A hearing aid or similar device being used to correct subnormal hearing to not better than normal.” Mo. Stat. § 542.200(5).

79. “Contents,” “when used with respect to any wire communication, includes any information concerning the identity of the parties, the substance, purport, or meaning of that

communication.” Mo. Stat. § 542.200(3).

80. An “Aggrieved person” is defined as “a person who was a party to any intercepted wire communication or a person against whom the interception was directed.” Mo. Stat. § 542.200 (1).

81. Zillow is a “Person” for purposes of the Act because it is a corporation.

82. Session Replay Code like that operated and employed at Zillow’s direction is an “electronic, mechanical or other device” used to transcribe electronic communications and to intercept a wire communication within the meaning of the Act.

83. The Session Replay Providers are not a party to the Website Communications—Plaintiff and the Classes only knew they were communicating with Zillow, not the Session Replay Providers.

84. Plaintiff’s and Class and Subclass members’ intercepted Website Communications constitute wire communications within the meaning of the Act.

85. Zillow intentionally operated and employed Session Replay Code on its website to spy on, automatically and secretly, and intercept its website visitors’ private electronic interactions communications with Zillow in real time, which are Contents within the meaning of the Act.

86. Plaintiff’s and Class and Subclass members’ private electronic communications were intercepted contemporaneously with their transmission.

87. Plaintiff and members of the Classes had a reasonable expectation of privacy in their Website Communications based on the detailed information the Session Replay Code collected from Plaintiff and members of the Classes.

88. Plaintiff and members of the Classes did not consent to having their Website Communications surreptitiously intercepted and recorded and are Aggrieved persons within the

meaning of the Act.

89. Pursuant to Mo. Stat. § 542.418, Plaintiff and members of the Classes are entitled to: (1) actual damages; (2) statutory damages including liquidated damages at \$100 per day of violation or \$10,000, whichever is greater, and (3) punitive damages. Plaintiff is also entitled to an award of attorney’s fees and expenses.

90. Zillow’s conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and members of the Classes any time they visit Defendant’s website with Session Replay Code enabled without their consent. Plaintiff and members of the Classes are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT II
Violation of Missouri’s Merchandising Practices Act
Mo. Rev. Stat. § 407.010 *et seq.*

91. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

92. Plaintiff brings this claim individually and on behalf of the Classes.

93. The Missouri Merchandising Practice Act (for the purposes of this section, “MPA”) protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

94. The Missouri MPA makes unlawful the “act, use or employment by any person of any deception, fraud, false pretense, misrepresentation, unfair practice, or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce.” Mo. Rev. Stat. § 407.020.

95. Plaintiff, individually and on behalf of the Classes, is entitled to bring this action pursuant to Mo. Rev. Stat. § 407.025, which provides in relevant part that: (a) Any person who purchases or leases merchandise primarily for personal, family or household purposes and thereby

suffers an ascertainable loss of money or property, real or personal, as a result of the use or employment by another person of a method, act or practice declared unlawful by section 407.020, may bring a private civil action in either the circuit court of the county in which the seller or lessor resides or in which the transaction complained of took place, to recover actual damages. The court may, in its discretion, award to the prevailing party attorney's fees, based on the amount of time reasonably expended, and may provide such equitable relief as it deems necessary or proper.

96. Zillow is a “person” within the meaning of the Mo. Rev. Stat. § 407.010(5) in that Zillow is a domestic “[...] for-profit [...] corporation.”

97. Plaintiffs and members of the Classes are “persons” under the MPA in that they are natural person or a natural person's legal representative, and they visited www.zillow.com to utilize the Zillow search engine for personal, family, and/or household use. Furthermore, Plaintiff Jill Adams visited www.zillow.com to utilize the Zillow search engine to shop for, purchase, and/or contract to purchase “merchandise”—real estate—for personal, family, and/or household use. Plaintiff Jill Adams also downloaded and used the Zillow App for personal, family, and/or household purposes.

98. The MPA applies to Zillow's conduct described herein because it protects consumers in transactions that are intended to result, or which have resulted in the sale of goods or services.

99. The MMPA defines “merchandise” as any objects, wares, goods, commodities, intangibles, real estate, or services. *See* Mo. Rev. Stat. § 407.010. Thus, the real estate search engine regarding millions of for-sale and rental listings, the Zestimate® home value service, and/or local professionals connector are services that Zillow provides to its website visitors are merchandise within the meaning of the Act. Plaintiffs and members of the class also

received Zillow’s offer to use a search engine and/or look at a Zestimate and accepted that offer by using the search engine and/or looking at a Zestimate under the act, relying on the Terms of Use of the Website.

100. “Trade” or “commerce” is defined as “the advertising, offering for sale, sale, or distribution, or any combination thereof, of any services and any property, tangible or intangible, real, personal, or mixed, and any other article, commodity, or thing of value wherever situated.” Zillow’s advertising, offering for sale, and sale of its real estate search engine and the real estate located thereon on www.zillow.com is considered “trade” or “commerce” in the State of Missouri within the meaning of Mo. Rev. Stat. § 407.010(7).

101. The Missouri Attorney General has promulgated regulations defining the meaning of unfair practice as used in the above statute. Specifically, Mo. Code Regs. tit. 15, § 60-8.020, provides:

(1) An unfair practice is any practice which—

(A) Either—

1. Offends any public policy as it has been established by the Constitution, statutes or common law of this state, or by the Federal Trade Commission, or its interpretive decisions; or

2. Is unethical, oppressive or unscrupulous; and

(B) Presents a risk of, or causes, substantial injury to consumers.

(2) Proof of deception, fraud, or misrepresentation is not required to prove unfair practices as used in section 407.020.1., RSMo. (*See, Federal Trade Commission v. Sperry and Hutchinson Co.*, 405 U.S. 233, 92 S.Ct. 898, 31 L.Ed.2d 170 (1972); *Marshall v. Miller*, 302 N.C. 539, 276 S.E.2d 397 (N.C. 1981); *see also*, Restatement, Second, Contracts, sections 364 and 365).

102. Pursuant to Mo. Rev. Stat. §407.020 and Mo. Code Regs. Tit. 15, § 60- 8.020, Defendant's acts and omissions fall within the meaning of "unfair."

103. Missouri case law provides that the MMPA's "literal words cover *every practice imaginable and every unfairness to whatever degree.*" *Conway v. CitiMortgage, Inc.*, 438S.W.3d 410, 416 (Mo. 2014) (quoting *Ports Petroleum Co., Inc. of Ohio v. Nixon*, 37 S.W.3d237, 240 (Mo. banc 2001). Furthermore, the statute's "plain and ordinary meaning of the words themselves . . . are unrestricted, all-encompassing and exceedingly broad." *Id.* at 240.

104. Zillow violated the MPA by omitting and/or concealing material facts about www.zillow.com and/or engaging in unfair or deceptive trade practices in its operation of www.zillow.com. Notably, Zillow omitted and/or concealed that it directed Session Replay Providers to secretly monitor, collect, transmit, and discloses its website visitors' Website Communications to the Session Replay Providers using Session Replay Code.

105. Zillow's direction and employment of the Session Replay Providers and their Session Replay Codes to intercept, collect, and disclose website visitors' Website Communications are material to the transactions on www.zillow.com. Zillow is leading online residential real estate marketplace in the United States and Zillow does not disclose its use of Session Replay Code to secretly monitor and collect website visitors' Website Communications. Had Plaintiff and the members of the Classes known that the Session Replay Codes (that collect, transmit, and disclose Website Communications to the Session Replay Providers) were embedded in Zillow's website, they would not have visited www.zillow.com to shop for, purchase, or contract to purchase real estate or they would have required Zillow to compensate them for the interception, collection, and disclosure of their Website Communications.

106. Zillow intentionally concealed the interception, collection, and disclosure of

website visitors’ Website Communications using Session Replay Code embedded in www.zillow.com is material because it knows that consumers would not otherwise visit its website to search for, purchase, and contract to purchase real estate. Indeed, Zillow’s concealment of such facts was intended to mislead consumers.

107. Zillow’s concealment, suppression, and/or omission of material facts was likely to mislead reasonable consumers under the circumstances, and thus constitutes an unfair and deceptive trade practice in violation of the MPA.

108. By failing to disclose and inform Plaintiff and the Classes about its interception, collection, and disclosure of website visitors’ Website Communications, Zillow engaged in acts and practices that constitute unlawful practices in violation of Mo. Ann. Stat. §§ 407.010, *et seq.*

109. As a direct and proximate result of these unfair and deceptive practices, Plaintiff and each member of the Classes has suffered actual harm in the form of money and/or property because the disclosure of their Website Communications has value as demonstrated by the collection and use of it by Zillow. The collection and use of this information has now diminished the value of such information to Plaintiff and the Classes.

110. As such, Plaintiff and the Classes seek an order (1) requiring Zillow to cease the unfair practices described herein; (2) awarding actual damages; and (3) awarding reasonable attorneys’ fees and costs. Plaintiff and the Classes seek all relief available under Mo. Ann. Stat. § 407.020, which prohibits “the act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce...,” as further interpreted by Mo. Code Regs. Ann. tit. 15, §§ 60-7.010, *et seq.*, Mo. Code Regs. Ann. tit. 15, §§ 60-8.010, *et seq.*, and Mo. Code Regs. Ann. tit. 15, §§ 60-9.010,

et seq., and Mo. Ann. Stat. § 407.025, which provides for the relief sought in this count.

111. Zillow’s conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and members of the Classes any time they visit Defendant’s website with Session Replay Code enabled without their consent. Plaintiff and members of the Classes are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT III

Invasion of Privacy – Intrusion Upon Seclusion

112. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

113. Under Missouri law, the general tort of invasion of privacy describes four distinct torts under Missouri law: (1) unreasonable intrusion upon the seclusion of another; or (2) appropriation of the other's name or likeness; or (3) unreasonable publicity given to the other's private life; or (4) publicity that unreasonably places the other in a false light before the public. Plaintiff brings this claim individually and on behalf of the Classes. Plaintiff states a claim for unreasonable intrusion upon the seclusion of another.

114. Plaintiff and members of the Classes had an objective, reasonable expectation of privacy in their Website Communications.

115. Plaintiff and members of the Classes did not consent to, authorize, or know about Zillow’s intrusion at the time it occurred. Plaintiff and members of the Classes never agreed that Zillow could collect or disclose their Website Communications.

116. Plaintiff and members of the Classes had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

117. Zillow intentionally intruded on Plaintiff's and Class and Subclass members' private life, seclusion, or solitude, without consent.

118. Zillow's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

119. Plaintiff and members of the Classes were harmed by Zillow's wrongful conduct as Zillow's conduct has caused Plaintiff and the Classes mental anguish and suffering arising from their loss of privacy and confidentiality of their electronic communications.

120. Zillow's conduct has needlessly harmed Plaintiff and the Classes by capturing intimately personal facts and data in the form of their Website Communications. This disclosure and loss of privacy and confidentiality has caused Plaintiff and the Classes to experience mental anguish, emotional distress, worry, fear, and other harms.

121. Additionally, given the monetary value of individual personal information, Defendant deprived Plaintiff and members of the Classes of the economic value of their interactions with Defendant's website, without providing proper consideration for Plaintiff's and Class and Subclass members' property.

122. Further, Zillow has improperly profited from its invasion of Plaintiff and Class and Subclass members' privacy in its use of their data for its economic value.

123. As a direct and proximate result Zillow's conduct, Plaintiff and members of the Classes are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

124. Zillow's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and members of the Classes any time they visit Defendant's website with session replay software enabled without their consent. Plaintiff and members of the Classes

are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

REQUEST FOR RELIEF

Plaintiff, individually and on behalf of the other members of the proposed Classes, respectfully requests that the Court enter judgment in Plaintiffs' and the Classes' favor and against Defendant as follows:

- A. Certifying the Class and appointing Plaintiff Jill Adams, herself, and Jill Adams in her capacity as Natural Mother and Next Friend of her minor child, H.A., as representatives of the Class;
- B. Certifying the Subclass and appointing Plaintiff Jill Adams in her capacity as Natural Mother and Next Friend of her minor child, H.A., as representative of the Subclass;
- C. Appointing Plaintiff's counsel as class counsel;
- D. Declaring that Defendant's past conduct was unlawful, as alleged herein;
- E. Declaring Defendant's ongoing conduct is unlawful, as alleged herein;
- F. Enjoining Defendant from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;
- G. Awarding Plaintiff and the Classes statutory, actual, compensatory, consequential, punitive³⁰, and nominal damages, as well as restitution and/or disgorgement of profits

³⁰ Recent changes to the Missouri Merchandising Practices Act (MMPA) provide that:

A claim for punitive damages shall not be contained in the initial pleading and may only be filed as a written motion with permission of the court no later than 120 days prior to the final pretrial conference or trial date. The written motion for punitive damages must be supported by evidence. The

unlawfully obtained;

H. Awarding Plaintiff and the Classes pre-judgment and post-judgment interest;

I. Awarding Plaintiff and the Classes reasonable attorneys' fees, costs, and expenses;

and

J. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the Class, demands a trial by jury of any and all issues in this action so triable of right.

Dated: September 27, 2022

Respectfully submitted,

/s/ Tiffany Marko Yiatras
Tiffany Marko Yiatras, MOED Bar No. 58197MO
CONSUMER PROTECTION LEGAL, LLC
308 Hutchinson Road
Ellisville, Missouri 63011-2029
Tele: 314-541-0317
Email: tiffany@consumerprotectionlegal.com

Bryan L. Bleichner (MN #0326689), to seek
admission *pro hac vice*
CHESTNUT CAMBRONNE PA
100 Washington Avenue S, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com

amount of punitive damages shall not be based on harm to nonparties. A pleading seeking a punitive damage award may be filed only after the court determines that the trier of fact could reasonably conclude that the standards for a punitive damage award, as provided in the act, have been met. The responsive pleading shall be limited to a response of the newly amended punitive damages claim.

Thus, Plaintiffs expressly disclaim punitive damages in this initial pleading; however, expect to file as a written motion with permission of the Court no later than 120 days prior to the final pretrial conference or trial date seeking punitive damages.

Kate M. Baxter-Kauf (MN #0392037), to seek admission *pro hac vice*

Karen Hanson Riebel (MN #0219770), to seek admission *pro hac vice*

LOCKRIDGE GRINDAL NAUEN P.L.L.P.

100 Washington Avenue South, Suite 2200

Minneapolis, MN 55401

Telephone: (612) 339-6900

Facsimile: (612) 339-0981

kmbaxter-kauf@locklaw.com

khriebel@locklaw.com

Attorneys for Plaintiff and the putative Class

[Query](#) [Reports](#) [Utilities](#) [Help](#) [Log Out](#)

**U.S. District Court
Eastern District of Missouri (St. Louis)
CIVIL DOCKET FOR CASE #: 4:22-cv-01023-JAR**

Adams et al v. Zillow Group, Inc.
Assigned to: District Judge John A. Ross
Demand: \$5,000,000
Cause: 28:1332 Diversity-Breach of Contract

Date Filed: 09/27/2022
Jury Demand: Plaintiff
Nature of Suit: 195 Contract Product Liability
Jurisdiction: Diversity

Plaintiff

Jill Adams

represented by **Tiffany M. Yiatras**
CONSUMER PROTECTION LEGAL
308 Hutchinson Road
Ellisville, MO 63011
314-541-0317
Fax: 855-710-7706
Email:
tiffany@consumerprotectionlegal.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

Jill Adams

*as Natural Mother and Next Friend of her
minor child, individually and on behalf of
all others similarly situated
next friend
H.A.*

represented by **Tiffany M. Yiatras**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

V.

Defendant

Zillow Group, Inc.

Date Filed	#	Docket Text
09/27/2022	<u>1</u>	COMPLAINT against defendant Zillow Group, Inc. with receipt number AMOEDC-9527448, in the amount of \$402 Jury Demand,, filed by Jill Adams(individually and on behalf of all others similarly situated), Jill Adams(as Natural Mother and Net Friend of her minor child, H.A., individually and on behalf of all others similarly situated). (Attachments: # <u>1</u> Civil Cover Sheet, # <u>2</u> Original Filing Form, # <u>3</u> Summons Zillow Group, Inc.)(Yiatras, Tiffany) (Entered: 09/27/2022)
09/27/2022	<u>2</u>	NOTICE OF PROCESS SERVER by Plaintiffs Jill Adams, Jill Adams (Yiatras, Tiffany) (Entered: 09/27/2022)
09/27/2022		Case Opening Notification. Judge Assigned: Honorable Shirley P. Mensah. 1 Summons(es)

		issued and emailed to Tiffany M. Yiatras. All parties must file the Notice Regarding Magistrate Judge Jurisdiction Form consenting to or opting out of the Magistrate Judge jurisdiction. Click here for the instructions. All non-governmental organizational parties (corporations, limited liability companies, limited liability partnerships) must file a Disclosure of Organizational Interests Certificate within 10 days of the filing of the first pleading or entry of appearance (moed-0001.pdf). (JBH) (Entered: 09/27/2022)
09/27/2022	3	AMENDED NOTICE OF PROCESS SERVER by Plaintiffs Jill Adams, Jill Adams Process Server: Northshore Process Legal Support Services, Inc. (Yiatras, Tiffany) Modified on 9/28/2022 (JEB). (Entered: 09/27/2022)
09/27/2022	4	Pursuant to Local Rule 2.08, the assigned/referred magistrate judge is designated and authorized by the court to exercise full authority in this assigned/referred action or matter under 28 U.S.C. Sec. 636 and 18 U.S.C Sec. 3401, including any case budgeting matters. (Potter, Jacob) (Entered: 09/27/2022)
10/14/2022	5	CJRA ORDER (GJL). Magistrate Judge Shirley Padmore Mensah termed. Case reassigned to District Judge Ronnie L. White for all further proceedings. (HMA) (Entered: 10/14/2022)
10/17/2022	6	Electronic Notice re: Disclosure of Organizational Interests Certificate to Defendant Zillow Group, Inc.. Pursuant to Local Rule 2.09, every non-governmental organizational party must file a Disclosure of Organizational Interests Certificate within ten (10) days of the party's first pleading or entry of appearance. Please complete and file the certificate as soon as possible (moed-0001.pdf). (Disclosure of Organizational Interests Certificate due by 10/27/2022.) (TMT) (Entered: 10/17/2022)
10/17/2022	7	ORDER: IT IS HEREBY ORDERED that this case is transmitted to the Clerk of the Court for random reassignment. Signed by District Judge Ronnie L. White on 10/17/2022. (TMT) (Entered: 10/17/2022)
10/17/2022	8	REASSIGNMENT ORDER (GJL). District Judge Ronnie L. White no longer assigned to case. Case reassigned to District Judge John A. Ross for all further proceedings. (TMT) (Entered: 10/17/2022)

PACER Service Center			
Transaction Receipt			
10/19/2022 10:44:51			
PACER Login:	samanthasouthall	Client Code:	0106198-000001-SS
Description:	Docket Report	Search Criteria:	4:22-cv-01023-JAR
Billable Pages:	2	Cost:	0.20

**BEFORE THE
UNITED STATES JUDICIAL PANEL
ON MULTIDISTRICT LITIGATION**

**In re: ZILLOW GROUP, INC. SESSION
REPLAY SOFTWARE LITIGATION**

MDL-__

CORRECTED SCHEDULE OF ACTIONS

	Case Caption	Court	Civil Action No.	Judge
1.	Plaintiff: Jamie Huber Defendant: Zillow Group, Inc.	United States District Court for the Eastern District of Pennsylvania	2:22-cv-03572	The Honorable Gerald J. Pappert
2.	Plaintiff: Ryan Margulis Defendant: Zillow Group, Inc.	United States District Court for the Northern District of Illinois – Eastern Division	1:22-cv-04847	The Honorable Edmond E. Chang
3.	Plaintiff: Ashley Popa Defendant: Zillow Group, Inc.	United States District Court for the Western District of Pennsylvania	2:22-cv-01287	The Honorable William S. Stickman, IV
4.	Plaintiffs: Natalie Perkins and Kenneth Hasson Defendants: Zillow Group, Inc. and Microsoft Corporation	United States District Court for the Western District of Washington	2:22-cv-01282	The Honorable Richard A. Jones
5.	Plaintiff: David Kauffman Defendant: Zillow Group, Inc.	United States District Court for the Southern District of California	3:22-cv-01398	The Honorable Linda Lopez
6.	Plaintiff: Jill Strelzin Defendant: Zillow Group, Inc.	United States District Court for the Northern District of Illinois – Eastern Division	1:22-cv-05644	The Honorable Steven C. Seeger

	Case Caption	Court	Civil Action No.	Judge
7.	Plaintiffs: Mark Conlisk and Michael Dekhtyar Defendant: Zillow Group, Inc.	United States District Court for the Northern District of Illinois – Eastern Division	1:22-cv-05082	The Honorable John F. Kness
8.	Plaintiffs: Jill Adams Jill Adams as Natural Mother and Next Friend of her minor child, H.A. Defendant: Zillow Group, Inc.	United States District Court for the Eastern District of Missouri	4:22-cv-01023	The Honorable John A. Ross

Dated: October 20, 2022

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

By: /s/ Samantha L. Southall

Samantha L. Southall
Two Liberty Place
50 S. 16th Street, Suite 3200
Philadelphia, Pennsylvania 19102
(215) 665-8700
samantha.southall@bipc.com

Christopher J. Dalton
550 Broad Street, Suite 810
Newark, New Jersey 07102-4582
(973) 273-9800
christopher.dalton@bipc.com

Jennifer Olmedo-Rodriguez
One Biscayne Tower
2 S. Biscayne Blvd., Suite 1500
Miami, Florida 33131
(305) 347-5900
jennifer.olmedo-rodriguez@bipc.com

Counsel for Zillow Group, Inc.

**BEFORE THE
UNITED STATES JUDICIAL PANEL
ON MULTIDISTRICT LITIGATION**

**In re: ZILLOW GROUP, INC. SESSION
REPLAY SOFTWARE LITIGATION**

MDL-__

CORRECTED PROOF OF SERVICE

Pursuant to JPML Rule 4.1(a), I certify that the foregoing documents were served via e-mail and regular US mail on the following:

Ari H. Marcus, Esquire
MARCUS & ZELMAN LLC
701 Cookman Avenue, Suite 300
Asbury Park, NJ 07712
ari@marcuszelman.com

*Counsel for Plaintiff Jamie Huber and the
Putative Class*

Douglas A. Millen, Esquire
Michael E. Moskovitz, Esquire
FREED KANNER LONDON
& MILLEN LLC
2201 Waukegan Road, Ste. 130
Bannockburn, IL 60015
(224) 632-4500
dmillen@fkmlaw.com
mmoskovitz@fkmlaw.com

*Counsel for Plaintiff Ryan Margulis and the
Putative Class*

Jonathan M. Jagher, Esquire
FREED KANNER LONDON
& MILLEN LLC
923 Fayette Street
Conshohocken, Pennsylvania 19428
jjagher@fkmlaw.com

*Counsel for Plaintiff Ryan Margulis and the
Putative Class*

Gary Lynch, Esquire
Kelly K. Iverson, Esquire
Jamisen A. Etzel, Esquire
Elizabeth Pollock-Avery, Esquire
Nicholas A. Colella, Esquire
Patrick D. Donathen, Esquire
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
gary@lcllp.com
kelly@lcllp.com
jamisen@lcllp.com
elizabeth@lcllp.com
nicke@lcllp.com
patrick@lcllp.com

*Counsel for Plaintiff Ashley Popa and the
Putative Class*

*Counsel for Plaintiff Jill Strelzin and the
Putative Class*

*Counsel for Plaintiffs, Natalie Perkins and
Kenneth Hasson, and the Putative Class*

Joshua B. Swigart, Esquire
SWIGART LAW GROUP, APC
2221 Camino del Rio S., Suite 308
San Diego, CA 92108
Josh@SwigartLawGroup.com
*Counsel for Plaintiff David Kauffman and the
Putative Class*

Katrina Carroll, Esquire
Kyle Shamberg, Esquire
LYNCH CARPENTER LLP
111 W. Washington Street, Suite 1240
Chicago, IL 60602
katrina@lcllp.com
kyle@lcllp.com
*Counsel for Plaintiff Jill Strelzin and the
Putative Class*

Gary M. Klinger, Esquire
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
gklinger@milberg.com
*Counsel for Plaintiffs, Mark Conlisk and
Michael Dekhtyar, and the Putative Class*

Kim D. Stephens, P.S., Esquire
Jason T. Dennett, Esquire
Kaleigh N. Boyd, Esquire
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
kstephens@tousley.com
jdennett@tousley.com
kboyd@tousley.com
*Counsel for Plaintiffs, Natalie Perkins and
Kenneth Hasson, and the Putative Class*

Joseph P. Guglielmo, Esquire
Carey Alexander, Esquire
Ethan Binder, Esquire
SCOTT+SCOTT ATTORNEYS
AT LAW LLP
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169
jguglielmo@scott-scott.com
calexander@scott-scott.com
ebinder@scott-scott.com
*Counsel for Plaintiffs, Natalie Perkins and
Kenneth Hasson, and the Putative Class*

Daniel G. Shay, Esquire
LAW OFFICE OF DANIEL G. SHAY
2221 Camino del Rio S., Suite 308
San Diego, CA 92108
DanielShay@TCPAFDPCA.com
*Counsel for Plaintiff David Kauffman and the
Putative Class*

Nick Suci III
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
6905 Telegraph Road, Suite 115
Bloomfield Hills, MI 48301
nsuciu@milberg.com
*Counsel for Plaintiffs, Mark Conlisk and
Michael Dekhtyar, and the Putative Class*

E. Kirk Wood, Esquire
Sharika Robinson, Esquire
Marcela Jenkins, Esquire
WOOD LAW FIRM, LLC
P. O. Box 382434
Birmingham, AL 35238-2434
kirk@woodlawfirmllc.com
srobinson@sharikamrobinsonlaw.com
mar_mcdonough@hotmail.com
*Counsel for Plaintiffs, Natalie Perkins and
Kenneth Hasson, and the Putative Class*

Nicola Menaldo, Esquire
Anna M. Thompson, Esquire
PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101
NMenaldo@perkinscoie.com
AnnaThompson@perkinscoie.com
Counsel for Microsoft Corporation

James G. Snell, Esquire
PERKINS COIE LLP
3150 Porter Drive
Palo Alto, California 94304
JSnell@perkinscoie.com
Counsel for Microsoft Corporation

Charles B. Casper, Esquire
MONTGOMERY MCCracken WALKER
& RHOADS LLP
1735 Market Street, 21st Floor
Philadelphia, PA 19103
ccasper@mmwr.com
Counsel for Microsoft Corporation

Tiffany Marko Yiatras, Esquire
CONSUMER PROTECTION LEGAL, LLC
308 Hutchinson Road
Ellisville, Missouri 63011-2029
tiffany@consumerprotectionlegal.com
*Counsel for Plaintiff Jill Adams and the
Putative Class*

Bryan L. Bleichner, Esquire
CHESTNUT CAMBRONNE PA
100 Washington Avenue S, Suite 1700
Minneapolis, MN 55401
bbleichner@chestnutcambronne.com
*Counsel for Plaintiff Jill Adams and the
Putative Class*

Kate M. Baxter-Kauf, Esquire
Karen Hanson Riebel, Esquire
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
kmbaxter-kauf@locklaw.com
khriebel@locklaw.com
*Counsel for Plaintiff Jill Adams and the
Putative Class*

I certify that the foregoing documents were served on the following via First Class

Mail:

Clerk of Court
United States District Court for the Northern
District of Illinois – Eastern Division
Dirksen U.S. Courthouse
219 S. Dearborn Street
Chicago, IL 60604
Via First Class Mail Only

Clerk of Court
United States District Court for the Western
District of Washington
700 Stewart Street, Suite 2310
Seattle, WA 98101
Via First Class Mail Only

Clerk of Court
United States District Court for the Western
District of Pennsylvania
Joseph F. Weis, Jr. Courthouse
700 Grant Street
Pittsburgh, PA 15219
Via First Class Mail Only

Clerk of Court
United States District for the Eastern District
of Pennsylvania
James A. Byrne Courthouse
601 Market Street
Philadelphia, PA 19106
Via First Class Mail Only

Clerk of Court
United States District Court for the Eastern
District of Missouri
Thomas F. Eagleton Courthouse
111 South 10th Street
St. Louis, MO 63102
Via First Class Mail Only

Clerk of Court
United States District Court for the Southern
District of California
James M. Carter & Judith N. Keep
Courthouse
333 West Broadway, Suite 420
San Diego, CA 92101
Via First Class Mail Only

Dated: October 20, 2022

/s/ Samantha L. Southall
Samantha L. Southall